mossmann's blog

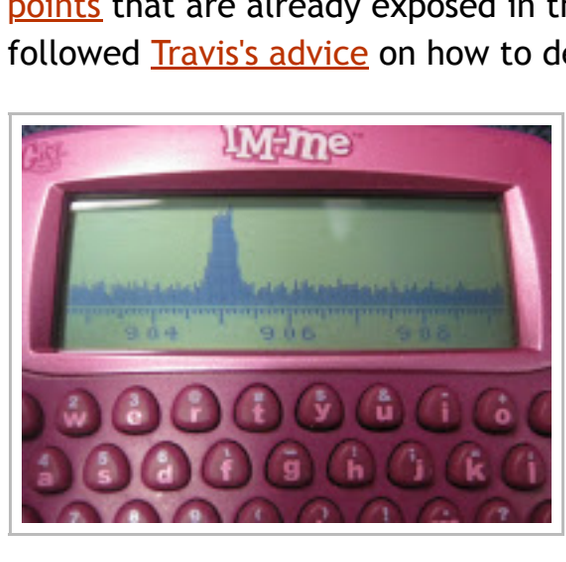
I am a terrible blogger

TUESDAY, MARCH 16, 2010

a $16 pocket spectrum analyzer

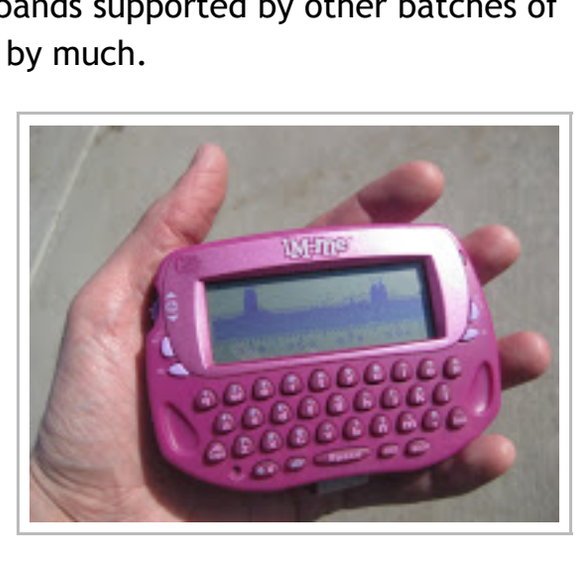
ShmooCon was, once again, a fantastic experience this year. One of many highlights of this year's event for me was hacking on some radio devices with Travis Goodspeed in the hotel bar for hours on end. This included playing with the IM-Me that he brought. As soon as I got home I ordered one. I found mine for $15.99 and free shipping on eBay.

Since then I've written custom firmware to turn my IM-Me into a pocket spectrum analyzer, shown here displaying activity of a frequency hopping system at a grocery store. The only change I've made to the hardware is the addition of a ribbon cable in order to easily connect to a GoodFET for programming, but this is simply creating a permanent connection to the debug contact points that are already exposed in the battery compartment. I've followed Travis's advice on how to develop for the platform.



The software tunes the IM-Me's radio chip to one frequency at a time, uses the chip's RSSI measurement function, and plots the result as one column on the LCD. It sweeps across the whole screen (132 columns) several times per second, showing a contiguous range of radio frequency activity. The technique works quite well, although there are a few defects. Most notably, harmonics of the IM-Me's 26 MHz crystal show up as spurs on the display.

The frequency ranges supported by my device are 281 - 361, 378 - 481, and 749 - 962 MHz. This is about 50% more than the chip is advertised to support and covers quite a bit of interesting activity in the US including ISM, LMR, television, amateur bands, pagers, and mobile phones. The edges of the bands supported by other batches of chips may differ but probably not by much.



The software supports three bandwidth modes: wide (default), narrow, and ultrawide. Wide mode displays 26.4 MHz of bandwidth in 200 kHz increments. Narrow mode displays 6.6 MHz of bandwidth in 50 kHz increments. Ultrawide mode, shown here with some mobile phone activity, displays 88 MHz of bandwidth in 667 kHz increments.

The code is open and available here. I'd love to hear from you if you give it a try. Huge thanks to both Travis and Dave who did the hard reverse engineering work!

Update: The code has a new home at github.

Posted by Michael Ossmann at 6:18 PM

Labels: imme, rf

28 comments:

Jared Boone said...

Beautiful work, Mike (and Travis and Dave). Repurposing mass-produced hardware and packaging for more interesting applications is so slick. I'm going shopping for a few IM-Mes, I think...

8:04 PM

Nate KI6STK said...

Hello, I am an amateur radio operator. Could this be tuned to a frequency and demodulated on the device to use as a receiver? and also, could an external antenna be used with the spectrum anylyzer?
Thanks, Nathanael.

10:39 AM

Michael Ossmann said...

Hey, Nate. Yes, demodulation can be done on the device for certain signals. Several variations of ASK and FSK are supported. See the cc1110 data sheet for details. It wouldn't be difficult to add an external antenna connector. The built-in antenna is a piece of wire (900 MHz quarter wave monopole) inside the case along the top of the LCD.

11:05 AM

bscogg said...

Hello everyone.

Do you think this would be possible with the original Zipit in the 2.4GHz spectrum? I have access to thousands at about this same price point.

Thanks in advance,
Brad

11:23 AM

Anonymous said...

Although you said that it supports bands at 200 or 300MHz, the balun network of the device is likely only meant for one of these bands. Is performance degraded by this?

12:27 PM

Michael Ossmann said...

Yes, the balun (not to mention the antenna) is designed for 900 MHz, so the lower bands do not perform as well. They also suffer more from internal interference. Still, I did some testing in all three bands, and it is useful even down at the low end.

I don't think a similar hack would be possible on the Zipit as it uses a 802.11 chip. If you find a device with a cc2530 or similar, though, let me know. :-)

12:51 PM

Sebastiano said...

Nice indeed Michael, I had been trying to refrain from buying a cheap IM-ME from ePay... don't think I'll succeed in refraining any longer now!

As to sporious response from the 26 MHz XTAL, wouldn't it be possible to implement a sort of calibration routine in software?

Something like:
- disable the antenna input of the radio IC
- measure exact frequency of the XTAL
- calculate exact harmonic freqs. of the XTAL
- measure RSSI outputs on those harmonic freqs. and write them to memory
- re-enable the antenna input of the radio IC
- at last modify the spectrum analyzer firmware so that the values of harmonics get subtracted from actual measurements taken on those same harmonics.

Just an idea, and beware that I'm no software engineer... so please don't laugh if this sounds as a dumb proposition.

Cheers,
S.

9:13 AM

Defaultito said...

Nice job Michael. I have ordered a IM-ME from ebay. But I wonder how to flash it with common tools/programmers. Any chance to program it using a PIC, AVR, or simmilar programmer? I'm not very familiarized with JTAG capabilities and GoodFET does not seem to be easily available. Any ideas?

Thank you!

5:29 PM

Michael Ossmann said...

I like the way you are thinking, Sebastiano, but there are drawbacks to your proposal.

If we normalize the output by subtracting the response without an antenna, then we show a reduced power level for signals at the same frequency as our spurs. For example, if we have a 10 dB spur from internal interference at 910 MHz and a 15 dB signal is detected, we would display it at 5 dB instead of 15 dB. You could argue that masking signals below 10 dB is also a problem, but at least there is an indication to the user that masking could occur. I'd rather have a visible defect than an invisible one. As an alternative, it might be worth trying to add some better internal shielding. The 26 MHz crystal is right next to the antenna path.

Frequency calibration would be nice too, but the only internal reference we have to measure the crystal is the crystal itself. It always appears to be perfect! We could calibrate to an external RF signal, but I haven't thought of a good one that would be available to most people. Something like WWVB would be nice, but it would have to be within the frequency range of the IM-Me.

Defaultito: I highly recommend the GoodFET. Travis is in the habit of handing out bare boards for free everywhere he goes (say, SOURCE Boston). The hardware is open source, so you could have boards printed yourself if you want. You could also build or buy a CC Flasher or a TI development kit. The serial debug protocol is well documented and could be implemented on other hardware. The Bus Pirate would be a good candidate. Travis's blog has some info that would be helpful if you wanted to try that.

10:45 PM

Defaultito said...

Thnak you Michael! Since I usually work with AVR, I will try to build a CC Flasher. It would be nice to have a yahoo group or forum for all interested in turn the IM-ME into a handheld spectrum analyzer. Many hams would be interested!

5:59 AM

Sebastiano said...

Michael, your points seem definetely reasonable.
Maybe XTAL harmonics could be reduced by removing the internal antenna (cutting PCB traces I suppose), and replacing it with a thin coax pigtail. Extra shielding for the XTAL would certainly help as well.
I'll have to experiment - in the end I surrendered to the temptation and ordered a cheap IM-ME :))
An external antenna connector would also be useful for connecting attenuators, signal generators etc.
Finally: a friend will be able to lend JTAG<->USB interfaces (based on Ark Pioneer or Prolific chips), I hope one of this interfaces will be able to load your firmware on the IM-ME.
I'll let you know....

7:14 AM

Hunter Davis said...

Hey Guys this is crazy impressive! Excellent hack! FYI there are some gpl drivers for the pc side of this device posted below

http://im-megpldrivers.sourceforge.net/

10:17 AM

Cybergibbons said...

Thanks for this work - I've just managed to get my IM-ME running this as well.

http://www.flickr.com/photos/cybergibbons/5162938944/

5:58 PM

Anonymous said...

Ewwww... What kind of person puts his grubby pocket device that's been god-knows-where on everyone's bell peppers like that?

4:22 PM

Anonymous said...

I assume the companion USB dongle also contains a CC1110 and that comparable tricks might be possible from the PC side?

9:28 PM

Michael Ossmann said...

I would have expected the dongle to contain a CC1111, but it has a CC1110. See Joby's blog for some great info.

10:25 PM

Lawz said...

Can this gizmo display FM analogue signals too, or just digitallly modulated signals?

11:09 AM

Michael Ossmann said...

Lawz: it will detect any radio signal in the supported frequency range. The modulation doesn't matter. I'm not doing any demodulation or decoding here.

9:25 PM

qrp-gaijin said...

Is this idea adaptable for HF? I'm thinking something like a mixer with a 280 MHz LO to convert the entire HF spectrum 0-30 MHz to 280-310 MHz, plus a lowpass filter to remove the image response. I'm interesed in measuring the harmonics of a homebrew 7 MHz CW rig.

Also, what's the dynamic range?

9:40 AM

conundrum said...

It ought to be possible to hack this for Wifi using a simple mixer and L.O. to downconvert the 2.4 to 2.5 GHz band (and for that matter any other band all the way up to 15 GHz i.e, satellite TV) into a suitable band.

Ghetto TCXO can be made using any old cheap 433MHz xtal or other oscillator, tap off the 2nd harmonic at 866 MHz and use temperature feedback circuit :-)

5:16 AM

conundrum said...

Sorry, that should be 3rd harmonic at 1732 MHz, leaving a difference frequency centred on 668 MHz at 2400 MHz and 768 MHz at 2500 MHz.

A simple tuned circuit bandpass filter would do the trick here.

5:29 AM

Anonymous said...

I want to build a POCSAG receiver from the im-me. This should be super fun.

3:29 AM

Gary Vk2kyp said...

Hi you please tell me which ebay dealer yu got your IM-Me from?
I am also aHam Radio operator
Thank you
regards Gary VK2KYP

12:51 AM

Gary Vk2kyp said...

Hi, can you please tell me the ebay seller you brought your IM-ME from? I am also a ham radio operator
regards Gary VK2KYP

12:55 AM

Xio Goering said...

Gary you can still buy it via Amazon, I just bought one.

Speaking of which I was curious if the device could be flashed with the bus pirate? The device is 3.3v tolerant, And I've wired it to my bp and been able to supply it power. However that's as far as I've gotten. Amy ideas?

11:11 AM

VK2WAR VK2WAR said...

Hi guys,

Now Im feeling left out!!! How brilliant you all are. Im looking for one myself. As an Aussie Ham Im crossing my fingers someone on Amazon will sell me one. (hard to find anyone on Amazon willing to ship to Australia).

Jason
VK2WAR.

7:20 PM

ddos said...

hi michele
i am very ig fan of u, will u plz send me deatild info on how to make rolljam and its bild instructions. i wil b very much thnak fll to you.

5:39 AM

Unknown said...

3:04 AM