By using our website and services, you expressly agree to the placement of our performance, functionality and advertising cookies. Learn more ACCEPT

Data logging Straightforward from the start data collection and display Technology

SPOOFING CELL NETWORKS WITH A USB TO VGA ADAPTER

by: Tom Nardi

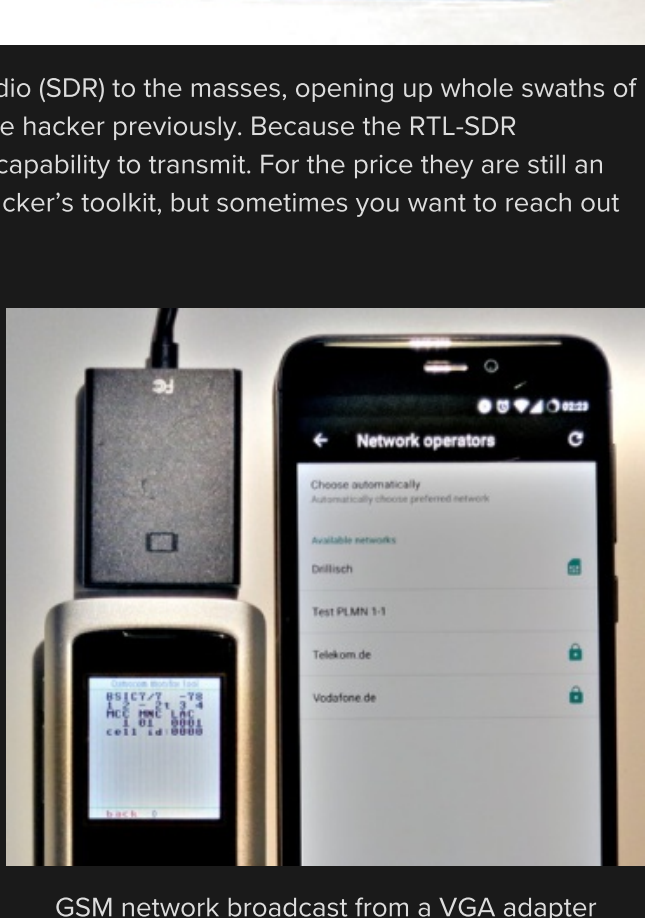
50 Comments

April 23, 2018

RTL-SDR brought cheap and ubiquitous Software Defined Radio (SDR) to the masses, opening up whole swaths of the RF spectrum which were simply unavailable to the average hacker previously. Because the RTL-SDR supported devices were designed as TV tuners, they had no capability to transmit. For the price they are still an absolutely fantastic deal, and deserve to be in any modern hacker's toolkit, but sometimes you want to reach out and touch someone.

Now you can. At OsmoDevCon [Steve Markgraf] released osmo-fl2k, a tool which allows transmit-only SDR through cheap USB 3.0 to VGA adapters based on the Fresco Logic FL2000 chip. Available through the usual overseas suppliers for as little has $5 USD, these devices can be used unmodified to transmit low-power FM, DAB, DVB-T, GSM, UMTS and GPS signals.

In a demonstration on the project page, one of these USB VGA adapters is used to broadcast a GSM cellular network which is picked up by the adjacent cell phones. Another example shows how it can be used to broadcast FM radio. A GitHub repository has been set up which includes more examples. The signals transmitted from the FL2000 chip are obviously quite weak, but the next step will logically be the hardware modifications necessary to boost transmission to more useful levels.


GSM network broadcast from a VGA adapter

To say this is a big deal is something of an understatement. For a few bucks, you'll be able to get a device to spoof cellular networks and GPS signals. This was possible before, of course, but took SDR hardware that was generally outside the budget of the casual experimenter. If you bought a HackRF or an Ettus Research rig, you were probably responsible enough not to get into trouble with it, but that's not necessarily the case anymore. As exciting as this technology is, we would be wise to approach it with caution. In an increasingly automated world, GPS spoofing can have some pretty bad results.

Posted in Radio Hacks, Slider, Software Hacks
Tagged osmo-fl2k, RTL-SDR, sdr, usb, vga

← The Simplest Possible DIY Ultrasonic Levitator

What Does 'Crypto' Actually Mean? →

pico Technology Data logging Straightforward from the start NEW PicoLog 6

50 THOUGHTS ON "SPOOFING CELL NETWORKS WITH A USB TO VGA ADAPTER"

Saabman says:
April 23, 2018 at 4:18 am

As things like this become more widespread. Security of online transactions becomes impossible for the average user. Will people stop using online services and go back to face to face transactions – is the openess of the internet the very thing that will kill it?

Reply Report comment

Fuzzyfuzzyfungus says:
April 23, 2018 at 4:44 am

I'm not sure why you'd identify this as the mechanism that breaks transaction security.

In non-doomed systems the authentication and encryption have treated the network connection as untrusted and potentially hostile for ages now; and any implementation that doesn't is toast the minute it hits an open wifi hotspot.

I suppose this makes grabbing SMS 'two factor' jokes slightly easier(at least for systems that will accept being downgraded to one of the old, vulnerable, cell standards, which is a bad idea though a common one); but those have always been bad practice and vulnerable via SS7 if not other means.

People already ignore much more serious threats to the integrity of a transaction to buy stuff online, this seems unlikely to deter them.

Reply Report comment

Zibri (@zibri) says:
April 23, 2018 at 8:07 am

I couldn't agree more than I do.

Reply Report comment

Saabman says:
April 23, 2018 at 7:04 pm

I don't see this as THE mechanism to "break" the internet but another mechanism to further reduce trust. Are we happy to continually chase our tails or just accept that we are just pawns in some global game… what we have is not ours to keep

Reply Report comment

kryptylomese says:
April 23, 2018 at 5:46 am

Backing up what Fuzzyfuzzyfungus said:-

https://www.schneier.com/blog/archives/2018/04/subverting_back.html

Reply Report comment

Maave says:
April 23, 2018 at 6:13 am

The internet is already tapped. Fortunately the heavy-hitters of the internet are pushing for encryption as default for everything.

Reply Report comment

Spacedog says:
April 23, 2018 at 7:20 am

I don't think the world is ready to pack up and go home. but we are in for a world of new wireless exploit discoveries for systems that operate in this devices extensive freq range. good time for researchers and repair technicians to replace all this insecure shit.

Reply Report comment

jonmayo says:
April 23, 2018 at 10:04 am

Honestly I could run secure transactions through unencrypted email if I wanted to. The physical layer network is not normally trustworthy, especially if it is wireless, and most reasonable protocols don't make too many assumptions about a link that can't be authenticated.

Until the classic Alice and Bob model presented by R.S.A. the industry was generally ignorant about the importance and capabilities of cryptographic protocols and authentication. Avoiding the man-in-the-middle attack has been a think for about 40 years now. Even if we don't always get it implemented right :-)

Reply Report comment

Andy Mc (@thisyearinbooks) says:
April 23, 2018 at 4:29 am

Anyone know of a dongle that has the correct chip in?

Reply Report comment

ItsThatIdiotAgain says:
April 23, 2018 at 4:49 am

"Anyone know of a dongle that has the correct chip in?"

I've bet my "about five bucks" on this one -> https://www.ebay.co.uk/itm/USB-3-0-to-VGA-Multi-display-Adapter-Converter-External-Video-Graphic-Cards-ED/132205650482?ssPageName=STRK%3AMEBIDX%3AIT&_trksid=p2057872.m2749.l2649
… based on nothing more than the description, price, and pictures.
I could of course be wrong. If so, you will still have an extra head for your laptop, so don't come back to me to complain.

Reply Report comment

presjar says:
April 23, 2018 at 4:55 am

This one should. The linked rar with driver files exe shows as fl2000

https://www.aliexpress.com/item/-/32806848832.html

Reply Report comment

elmesito says:
April 23, 2018 at 5:04 am

I recently bought this one so that I could have a 3rd screen. I can confirm it is a FL2000 . https://www.ebay.co.uk/itm/3-0-USB-to-VGA-Display-Cable-Video-Graphic-Adapter-For-Windows-7-8-10/132414331526?ssPageName=STRK%3AMEBIDX%3AIT&_trksid=p2060353.m2749.l2649

Reply Report comment

Andy Mc (@thisyearinbooks) says:
April 23, 2018 at 11:58 pm

You guys are awesome, thanks for the links.

Reply Report comment

Redhatter (VK4MSL) says:
April 23, 2018 at 4:33 am

Is this a quirk of this particular interface, or is it "the nature of the beast" due to a VGA interface requiring 3 high-speed DACs to produce high resolution graphics?

Reply Report comment

imroy264 says:
April 23, 2018 at 5:13 am

Perhaps a little of both.

Reply Report comment

fuzzyfuzzyfungus says:
April 23, 2018 at 1:07 pm

Some of both. Any implementation of VGA requires the pretty-impressive-for-the-money DACs; but 'smarter' implementations are more likely to include (normally helpful) features like framebuffers and automatic handling of vertical and horizontal blanking intervals that reduce your control over the output of the DACs. It will likely be as good or better for VGA, and with less effort on the software side(in this case, it looks like the fancy Displaylink stuff can handle markedly higher resolutions at equivalent bandwidth; and is actually somewhat useful on USB2, while the FL2000 just sneaks 1920×1080 in on USB3) ; but if you are trying to generate a signal that doesn't have horizontal and vertical blanks dumber is better, since the hardware won't even notice that you are blatantly violating the expectations of VGA in order to get what you want.

Reply Report comment

Alphatek says:
April 23, 2018 at 6:00 am

From a quick read, this chipset is useful because it doesn't have a local framebuffer, and streams direct from the host over USB (with associated problems…). It also allows VGA configs without H/V pulses, so can effectively spew a high speed raw datastream from host out the DACs.

Reply Report comment

rasz_pl says:
April 23, 2018 at 2:19 pm

I always wondered if Pee DPI parallel Video interface allowed 0 length blanking period, it seemed perfect for pumping data out at high speed, but this, this is even better!
8MB SPI chip on the pcb suggests FL2000DX to be programmable with a micro-controller inside :o Imagine what treasures lie there.
Wonder if its possible to wiggle H/V sync IO at 150MHz too. There is also provision for one more digital IO with missing Q3 on the board.

Universal triple >100 MS/s DAC at $5 is INSANE. Holy shit, $5 10MHz signal generators for everyone!

Are there any more chips like this in the wild? FX2LP was pretty revolutionary in its day, started out in USB 2.0 HDD enclosures, Cameras, digital tuners, ended up enabling low cost logic analyzer revolution.
I know of one more, quite old by now design from 2011, genesyslogic GL3220 used in multiple USB 3.0 multi card readers, capable of >100MB/s 8bit parallel transfers over its buildin UDMA7 CF interface. Available in $15 readers. Internally 8051.

Reply Report comment

2ftg says:
April 23, 2018 at 2:22 pm

If I have understood correctly that SPI flash is for the drivers.
So that you don't need to ship a CD with the dongle.
Still interesting, as is the VGA I2C interface.
I do expect tons of interesting projects to rise from this.

Reply Report comment

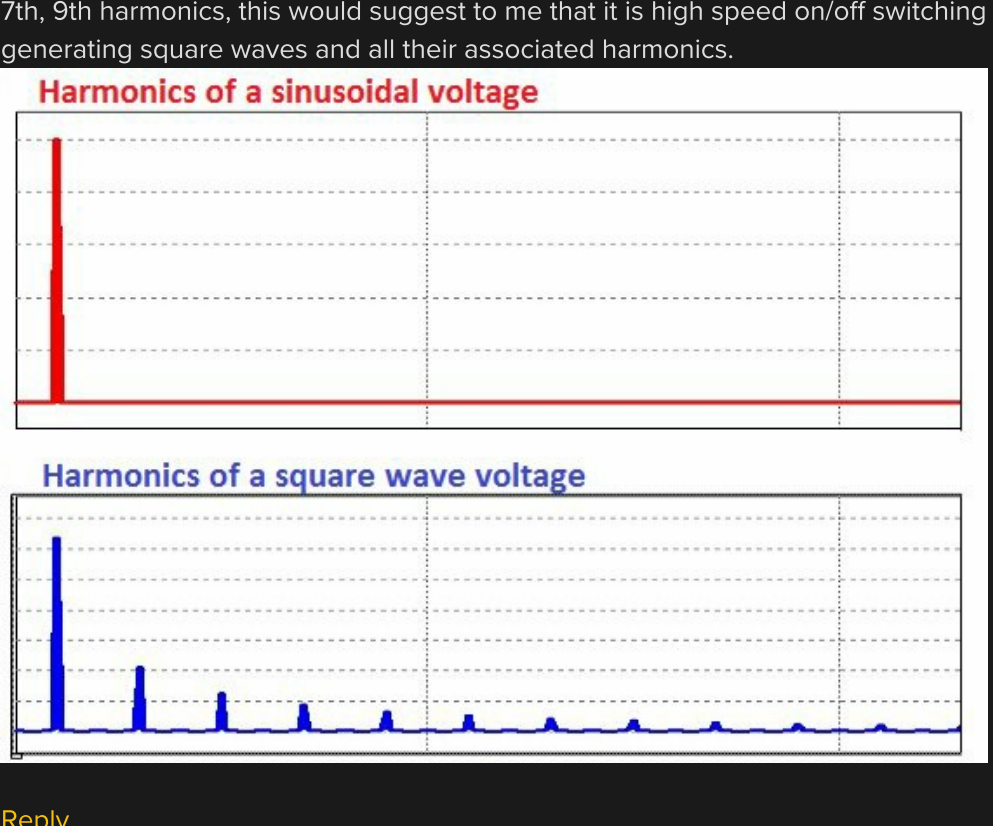
rasz_pl says:
April 23, 2018 at 4:16 pm

Yes, I found this out hour later while reading sources :(
still 3x 8bit (at least in theory) >100MHz DACs!
Cant wait for some tests with fast scope (jitter and actual number of bits).

Report comment

Truth says:
April 24, 2018 at 2:26 am

My guess is a delta sigma modulator. Because there is mention of the fundamental frequency, 3rd, 5th, 7th, 9th harmonics, this would suggest to me that it is high speed on/off switching which is in effect generating square waves and all their associated harmonics.



Reply Report comment

ItsThatIdiotAgain says:
April 23, 2018 at 4:35 am

Nice.. nest time that noisy reaper drone flies over the house and wakes up the cat, its getting planted straight into the local sewage farm. ;¬)

Reply Report comment

ItsThatIdiotAgain says:
April 23, 2018 at 4:36 am

/s/nest/next – … Actually on reflection, I might keep the reaper drone, I'm sure there must be a few useful bits and pieces in it.

Reply Report comment

Thinkerer says:
April 23, 2018 at 5:03 am

Likely the poor schmuck who's flying a 182 in slow circles around your city (while watching movies on his iPad), at least until the FAA approves UAVs in class B/C airspace.

https://www.buzzfeed.com/peteraldhous/spies-in-the-skies?utm_term=.gtNWzW1B6#.tik0D0mz5

Reply Report comment

Adam says:
April 23, 2018 at 4:40 am

Anyone got a link to the datasheet? A custom PCB with SMA connectors and amplifiers in is my future

Reply Report comment

Adam says:
April 23, 2018 at 4:40 am

Datasheet for the Fresco Logic FL2000

Reply Report comment

ItsThatIdiotAgain says:
April 23, 2018 at 4:52 am

"Datasheet for the Fresco Logic FL2000"
I've not found the FL2000 datasheet yet, but this might also be of interest -> https://github.com/FrescoLogic/FL2000

Reply Report comment

ItsThatIdiotAgain says:
April 23, 2018 at 5:06 am

Not much on the company web site…
Marketing blurb -> http://www.frescologic.com/product/single/fl2000
Support -> https://support.frescologic.com/portal/home
I'll do some more digging.

Reply Report comment

ItsThatIdiotAgain says:
April 23, 2018 at 4:57 am

"Anyone got a link to the datasheet? A custom PCB with SMA connectors and amplifiers in is my future"

For initial prototyping, or if the datasheet is not available, you could of course treat the FL2000 dongle as a "module" remove the VGA and USB connectors and solder it piggy back style to your custom board.

Reply Report comment

Ostracus says:
April 23, 2018 at 7:01 am

It's probably going to follow the same evolutionary path as the RTL-SDR.

Reply Report comment

phuzz says:
April 23, 2018 at 1:09 pm

I'm not so sure. I imagine that in a lot of jurisdictions it would be very difficult to sell something that could broadcast on restricted frequencies.

Reply Report comment

Martin says:
April 24, 2018 at 1:58 am

So you also want to control the sell of transistors, ferrite rods and magnet wire? This chip is not intended to broadcast. The reason the companys often keep the datasheet secret is first to avoid opening their know how (trade secrets) and often to avoid too much support calls from hobbyists.

Reply Report comment

w3axl says:
April 23, 2018 at 8:40 am

Honestly you could probably use the connector as-is. VGA signals are 75ohm and with a small matching pad you could easily break out the red+gnd signals to a 50ohm sma connector. That's what I'm planning on doing anyway.

Reply Report comment

MarSik OK7MS says:
April 23, 2018 at 9:27 am

Why not use the 75 ohm signals directly? All the digi TV coax is 75 ohm (lower losses and cheaper than 50 ohm coax here), dipoles are better matched to 75 ohms, BNCs are readily available for 75 ohms as well. In fact, most of my radio stuff is 75 ohms, because the power handling is not an issue for me.

Reply Report comment

Martin says:
April 24, 2018 at 2:00 am

Of course you can do that, if it fits your equipment. Probably even the mismatch is acceptable, if you use your 50 Ohm equipment. The 15pin sub D connector is not impedance controlled anyway.

Reply Report comment

mxb says:
April 23, 2018 at 4:53 am

The boxy one seems to match this model:
https://www.aliexpress.com/item/2colors-1080P-USB-3-0-to-VGA-Multi-Display-Video-Graphic-External-Cable-Adapter-Wire-for/32750625943.html

Reply Report comment

Thinkerer says:
April 23, 2018 at 5:00 am

So are we entering an era of homebrewed "Stingray" systems – this could get ugly.

Qui decipit spoofers?

Reply Report comment

2ftg says:
April 23, 2018 at 6:02 am

Those have been reality for more than a decade.
And this is just a transmitter without any return channel.
I'm unsure if it is even possible to make a GSM basestation with one of these and rtl-sdr.
That has not been possible even with two hackRF's and those are built to be SDR transceivers.
So the title is a bit clickbaity even if technically true.

Reply Report comment

cyk says:
April 23, 2018 at 5:10 am

Does anybody know, what the effective frequency range of this chip is?
I'm thinking of using it simply as a frequency generator, maybe with some additional functions like wobbling, comb generation, etc.

Reply Report comment

ItsThatIdiotAgain says:
April 23, 2018 at 5:39 am

"Does anybody know, what the effective frequency range of this chip is?
I'm thinking of using it simply as a frequency generator, maybe with some additional functions like wobbling, comb generation, etc."

"A typical 1920×1080@60 Hz requires 1920 * 1080 * 24bpp * 60 = 373,248,000 bytes/sec of traffic over the USB bus."

So we can be sure that the bandwidth is of that order of magnitude. i.e. 373.248MHz however since you can spoof cell phones, it must be greater than that, or at lest there is some clever trickery going on that makes it appear to be greater than that.

For more info, you will need to read the article linked above.

Reply Report comment

cyk says:
April 23, 2018 at 6:03 am

I didn't find what I was looking for at first, but this presentation shows how it's done:
http://people.osmocom.org/steve-m/fl2k_slides/osmo-fl2k.html#(1)

The basic frequency is 150MHz, and things like GSM, GPS, DVB-T use the harmonics.
fl2k_tcp streams samples form e.g. GnuRadio, so this can be used to transmit arbitrary waveforms.

Nice!

There are even plans to synchronize it with a rtl-sdr, to get an ultra cheap SDR transceiver.

Reply Report comment

2ftg says:
April 23, 2018 at 6:06 am

Well you get harmonics and as it's a DAC, you also get aliases at higher frequencies.
The GPS spoofing example is done with harmonics.

Reply Report comment

Oussema Harbi says:
April 23, 2018 at 6:17 am

btw : last year STM produced an STB with 2 WAYS communication with a satellite : i.e. satellite sends (ip ?) packets to the transponder on the actual satellite; they used the usual digital to analog converter and added an RF amplification stage instead of the RGB interface, kind of similar to what has been done here

Reply Report comment

Oussema Harbi says:
April 23, 2018 at 6:18 am

i.e. STB* sends …

Reply Report comment

some-ham says:
April 23, 2018 at 9:21 am

So looks like it is finally time where we can brew up a nice all in one poor ham full SDR; a preamp to an RTL and linear output from the FL with some good bandpass filtering.
We can start by prototyping it at low power with our Linux laptops but should quickly move to a cool does everything big handheld run by a capable ARM SCB with USB-3.0.
Imagine bringing well beyond the capabilities of those schmancy >$20K unobtanium Harris military radios into our hands for under $100!
Probably want some FPGAs to get fast encoding/decoding, change FPGA modes on the fly to change modes because we can with that tech.

Reply Report comment

Bill stewart says:
April 23, 2018 at 4:26 pm

It's really going to cost you a good bit more than $5, because you need a fast enough computer to do the job (plus it needs USB-C, though that's becoming available on cheap laptops by now. My work laptop doesn't have USB-C yet or I'd have to get one of these.)

Reply Report comment

Bill stewart says:
April 23, 2018 at 4:29 pm

Duh, cancel that – USB3 will do it even without USB-C. Now I have to go buy one, instead of just using the VGA connector on the docking station :-)

Reply Report comment

Frightened by Scary Things says:
April 24, 2018 at 1:43 am

Slightly twisted interpretation of what makes a responsible citizen, but then many will have been conditioned to agree.

Reply Report comment

herbert says:
April 24, 2018 at 3:16 am

responsible citizens do what they want so long as they do not restrict the freedom of others

Reply Report comment

Paul says:
April 24, 2018 at 2:23 am

How many people immediately ordered one after reading the original article, I certainly did.

Reply Report comment

Leave a Reply

Enter your comment here...

pico Technology Data logging Straightforward from the start NEW PicoLog 6

tindie CUTTING EDGE PRODUCTS MADE BY MAKERS

SEARCH

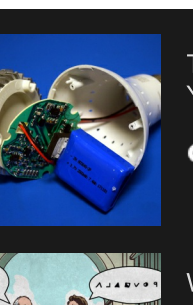
Search … SEARCH

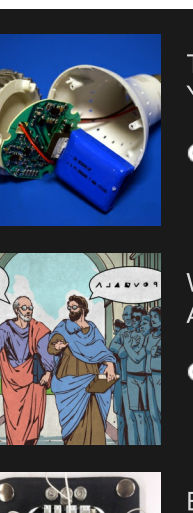
NEVER MISS A HACK

SUBSCRIBE

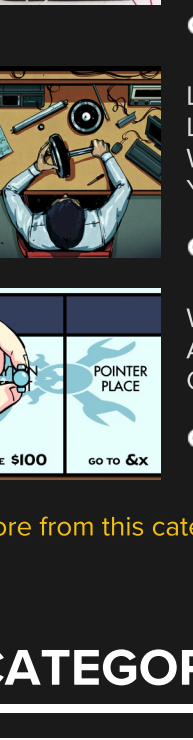
Enter Email Address SUBSCRIBE

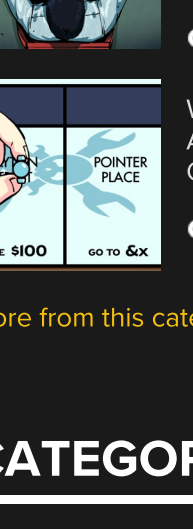
IF YOU MISSED IT


TEARDOWN: LED BULB YIELDS TINY UPS
52 Comments


WHAT DOES 'CRYPTO' ACTUALLY MEAN?
59 Comments

ETEXTILE SPRING BREAK TACKLES SIGNAL BLOCKING, AUDIO GENERATION, AND RADIO TRANSMISSIONS
12 Comments


LIFE ON CONTRACT: LOWERING YOUR COST WITHOUT DROPPING YOUR PRICE
14 Comments

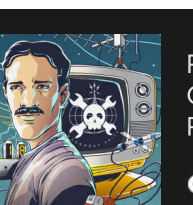

WHEN 4 + 1 EQUALS 8: AN ADVANCED TAKE ON POINTERS IN C
90 Comments

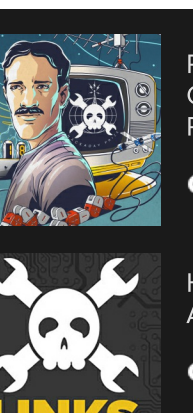
More from this category

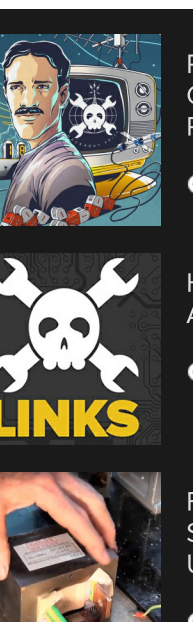
CATEGORIES

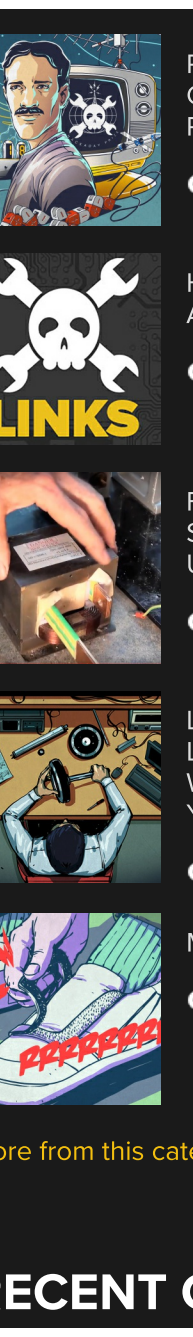
Select Category

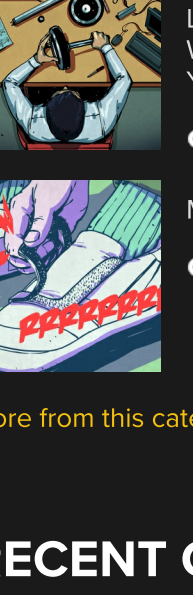
OUR COLUMNS


ROBOTICS MODULE CHALLENGE: BUILD ROBOT, WIN PRIZES
4 Comments


HACKADAY LINKS: APRIL 22, 2018
20 Comments


FAIL OF THE WEEK: THE SPOT WELDER UPGRADE THAT WASN'T
26 Comments


LIFE ON CONTRACT: LOWERING YOUR COST WITHOUT DROPPING YOUR PRICE
14 Comments


MECHANISMS: VELCRO
35 Comments

More from this category

RECENT COMMENTS

jwebola on What Does 'Crypto' Actually Mean?

gg on Margaret Hamilton Takes Software Engineering To the Moon and Beyond

herbert on 3000W Unicycle's Only Limitation Is "Personal Courage"

dave on Assemble Your Own Modular Li-Ion Batteries

John Dingley on 3000W Unicycle's Only Limitation Is "Personal Courage"

John Dingley on 3000W Unicycle's Only Limitation Is "Personal Courage"

herbert on Spoofing Cell Networks with a USB to VGA Adapter

herbert on What Does 'Crypto' Actually Mean?

John Dingley on 3000W Unicycle's Only Limitation Is "Personal Courage"

herbert on Tiny Vacuum Chamber Arm to Help with Homemade Semiconductors

NOW ON HACKADAY.IO

nikolaos liked Ferrofluid Sculptures .

Just4Fun has updated the log for ESP-01 NanoBoard (ESP8266).

lee has added a new project titled ヶ충남출장샵 【카톡:DG79C】충남출장만남 【주소GOLDEN，c0m】충남출장안마# 충남콜걸.

nate.damen has updated details to Altlvhead.

lee has added a new project titled ヨ울산출장샵 【카톡:DG79C】울산출장만남 【주소GOLDEN，c0m】울산출장안마# 울산콜걸.

lee has added a new project titled フ강원출장샵 【카톡:DG79C】강원출장만남 【주소GOLDEN，c0m】강원출장안마# 강원콜걸.

Neris has updated details to Increasing ADC resolution by nBits+1, Arduino AC.

Just4Fun has updated details to ESP-01 NanoBoard (ESP8266).

Yann Guidon / YGDES has updated details to Numitron Hexadecimal display module.

Varun Suresh has added Manoj Kumar as a contributor to NeuroCuddl.

pico Technology PicoLog 6 Data logging Straightforward from the start NEW Real-time data collection and display

Copyright © 2018 | Hackaday, Hack A Day, and the Skull and Wrenches Logo are Trademarks of Hackaday.com
Powered by WordPress.com VIP