

I want to see farther



*XFocus Team*

*www.xfocus.org*

*www.xfocus.net*

 X'con 2005

# Something you needed

## ◆ Devices

◆ Wifi Card

◆ Bluetooth Doggle

## ◆ Antennas

◆ Beam Antenna

◆ Omni Antenna

## ◆ Pigtail



I want to see farther



# Chose your wifi card

## ◆ Chipset & Compatibility

- ◆ Support monitor/master mode ?
- ◆ Support packet injection?
- ◆ Support linux ?
  - ◆ Ndiswrapper is great, but it's no help for us.
- ◆ Support Wireless Extensions ?



# Chose your wifi card

```
[root@TOMB tk]# iwlist wifi0 scanning
wifi0   Scan completed :
        Cell 01 - Address: 00:11:22:33:44:55
                ESSID:"research"
                Mode:Master
                Frequency:2.462 GHz (Channel 11)
                Quality:0/70  Signal level:-53 dBm  Noise level:-86 dBm
        .....
[root@TOMB tk]# iwlist eth1 scanning
eth1    Interface doesn't support scanning : Operation not supported
```



# Chose your wifi card

- ❖ Transmit Power
- ❖ Receiver Sensitivity
- ❖ Connector included ?
  - ❖ Easy to modify?



# Chose your wifi card

## ◆ 802.11b

### ◆ Prism Chipset

◆ Senao SL-2511CD PLUS EXT2

◆ ASUS WL100

### ◆ Realtek RT8180 Chipset

## ◆ 802.11g

### ◆ Atheros Chipset

### ◆ Ralink RT2500 Chipset



# Chose your wifi card

- ◆ Lucent Family
  - ◆ Agere(ORiNICO) & Avaya
  - ◆ OEMs
- ◆ Cisco Air-LMC350 Series
  - ◆ Air-LMC352
- ◆ Broadcom & TI Chipset



# Trap !

◆ Pay attention to Hardware Rev !

◆ eg: D-Link DWL-650

◆ DWL-650(A1-J3)

◆ DWL-650(K1)

◆ DWL-650(L1/L2/M1/P1)

◆ LinkSys WPC11、 SMC 2632W.....





# Chose your bluetooth

◆ Easy to modify?

◆ Transmit Power

- ◆ Class I      100mW(+20dBm)      100m
- ◆ Class II     2.5mW(+4dBm)      10m
- ◆ Class III    1mW(+0dBm)      1m

◆ Receiver Sensitivity

Power	Model	Manufacturer	Sensitivity
Class I	MS-6967	MSI	<b>-90 dBm</b>
Class I	BT3030	TECOM	-76 dBm
Class I	F8T001	Belkin	-80 dBm
Class I	BT-700	Acer	-70 dBm
Class I	USBBT100	LinkSys	-80 dBm
Class I	USBBTC1A	Billionton	-80 dBm



# Chose your bluetooth

## ◆ Compatibility

◆ CSR

◆ BroadCom

```
[tk@TOMB ~]$ sudo hciconfig hci0 features
```

```
hci0: Type: USB
```

```
BD Address: 00:11:12:33:44:55 ACL MTU: 128:8 SCO MTU: 64:8
```

```
Features: 0xff 0xff 0x05 0x00 0x00 0x00 0x00 0x00
```

```
<3-slot packets> <5-slot packets> <encryption> <slot offset>
```

```
<timing accuracy> <role switch> <hold mode> <sniff mode>
```

```
<park state> <RSSI> <channel quality> <SCO link> <HV2 packets>
```

```
<HV3 packets> <u-law log> <A-law log> <CVSD> <power control>
```



# Chose your antenna

## ✦ Enough gain

Gain (Sender)	Gain (Receiver)				
	18dBi	14dBi	8dBi	6dBi	5dBi
18dBi	3.4 miles	2.5 miles	1 mile	1100 yards	656 yards
14dBi	1.5 miles	1.5 miles	1 mile	874yards	656 yards
8dBi	1100 yards	1100 yards	1100 yards	874 yards	656 yards
6dBi	874 yards	874 yards	874 yards	874 yards	656 yards
5dBi	656 yards	656 yards	656 yards	656 yards	656 yards



# Chose your antenna

- ❖ Easy to take  
Easy to find
- ❖ Proper size  
Proper price



Arecibo, 305m



# Chose your antenna

- ❖ Hertz antenna
  - ❖ Half-Wave Dipole
- ❖ Marconi antenna
  - ❖ Quarter-Wave Monopole



# Chose your antenna

- ◆ Yagi Antenna
  - ◆ 10 dBi ~ 16 dBi
- ◆ "Flat Panel Antenna"
  - ◆ 5 dBi ~ 24 dBi
- ◆ Homemade Antenna
  - ◆ Good pastime
  - ◆ No bad gain



# Yagi Antenna

◆ Hidetsugu Yagi & Shintaro

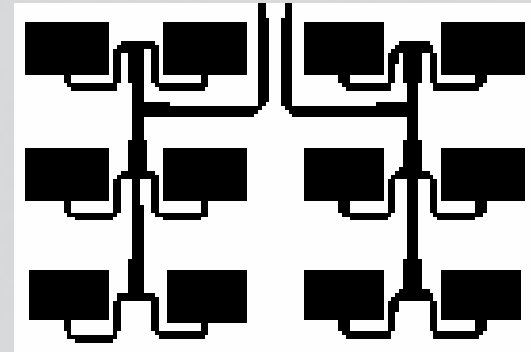
◆ Cheap price  
Acceptable size

◆ Medium gain



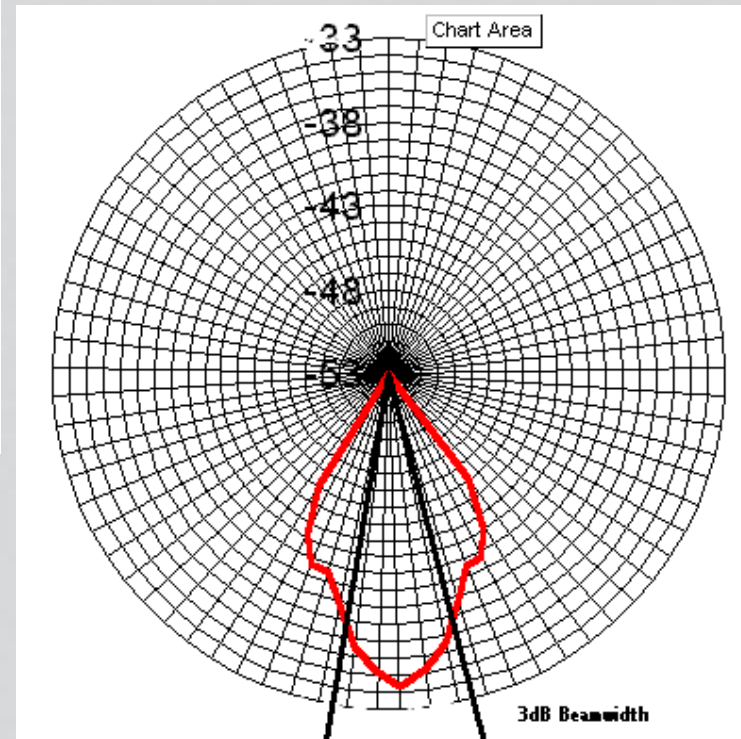
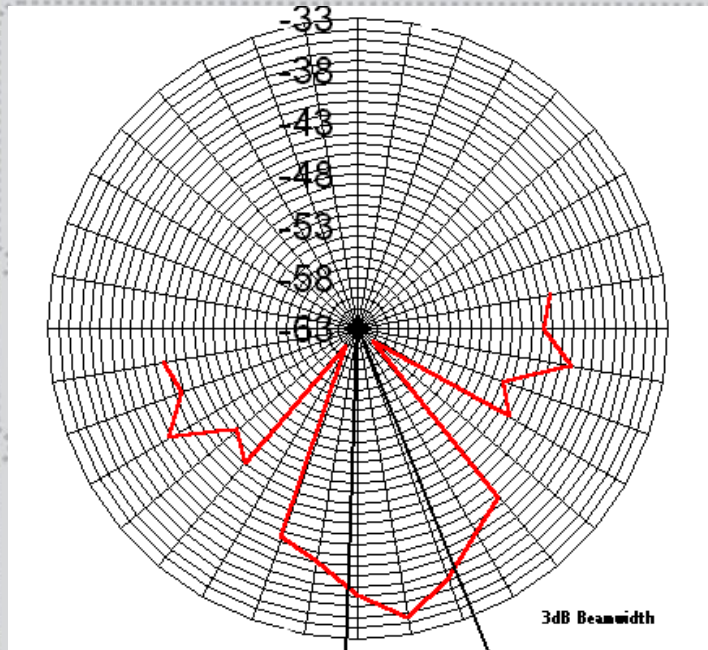
# “Flat Panel Antenna”

- ✦ Could more than 20dBi
- ✦ Portable
- ✦ Maybe expensive





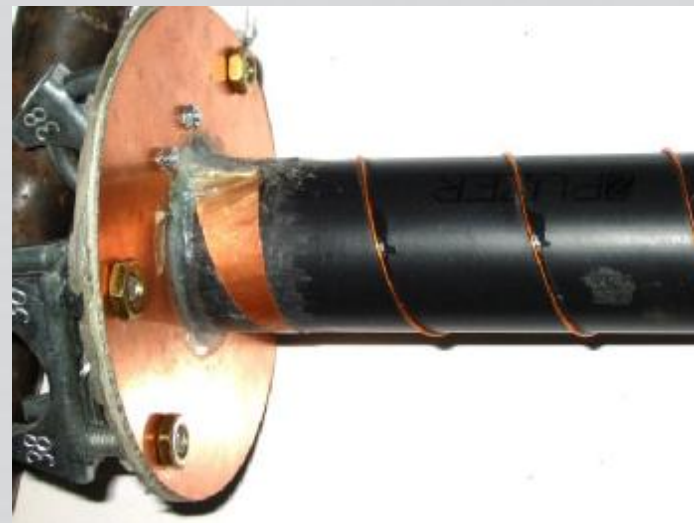
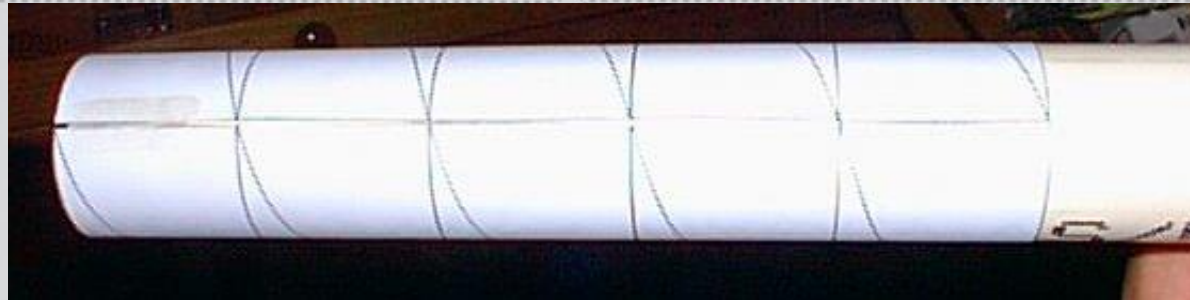
# Homemade Antenna



# Homemade Antenna



# Homemade Antenna



# Homemade Antenna



# Homemade Antenna



# Homemade Antenna



# Homemade Antenna



# Homemade Antenna





# Homemade Antenna



# Homemade Antenna



# Homemade Antenna



# Homemade Antenna

Must - certainly cost effective - NZ\$8! A 300mm diam (12") Chinese cooking vat scoop that closely approximates a shallow parabola. It's mesh holes (~5mm) are well under the min. .1 wavelength at 2.4GHz (1 wave = 125mm) & it gives little wind resistance & rust.

Diam = 300 mm, with 60mm depth  
(D) (c) to centre

$$f = \frac{D^2}{16c}$$

$$= \frac{300 \times 300}{16 \times 60}$$

$$= \frac{1500}{16}$$

So focus ~94mm out  
which is beyond most r.f. & may give weak signal pickup from sources not being looked at

f/D ratio desirably 0.25-0.55 for such 2.4GHz parabolas

Here = 94/300 = 0.31

This setup could look very professional / spray painted black & maybe mounted on a simple photographic tripod

Suitable support for the USB WiFi adaptor ( here a ~US\$40 "ZyDAS ED 1201" sold in NZ by DSE ) will of course be needed, maybe fed thru' the mesh from the back? USB dongle then can be removed until needed.

Parabolic reflective performance of amateur "appropriate technology" dishes can be quickly verified by Al foil curved around the mesh to direct the sun or a bright light to a focus

Experiments show mesh equiv. to "0.8" of a dish of similar size. Hence this equates to a solid dish 0.8 x 300 = 240mm & is likely to have gain ~15dB (A total of ~12dB!)

With one at each end of a link, the 30dB system gain could give ~10km LOS

Other simple DIY reflectors abound - with BBQ grill mesh likely better gain. Doubling dish diam gives 6dB gain & doubles range

POOR MANS WIFI?

Cheap & "lossless" long run (Cat) USB cables near reception "sweet spots" more easily exploited than normal costly microwave cable & connectors can justify. Over!

Sean Swan - MIU@W - 2nd May 2004  
=> s.t.swan@massey.ac.nz



# Homemade Antenna



# Homemade Antenna

Not your usual stir fry ! Here's a cheap wok from NZ's celebrated Warehouse, that's -parabolic !

s.t.wah@dmassey.ac.nz 25th May 04

With diam. 330mm & depth ~90mm it has a verified focal point ~75mm out. Being inside the rim this should gather signals well, & indeed performance looked superior (~17dB ?) beside the Scoop's ~15dB.

A hose mender again provides both USB cable protection & (when internally trimmed to suit) good support & standoff for the USB WiFi adaptor.



Handles will drill out if desired

A vitamin pill holder neatly fits over the USB adaptor if weather proofing needed

The chassis nibbler eases drilling out of the 25mm (1") mount hole. Recommended !



# Homemade Antenna

Since many PDAs, cell phones & IP Wireless devices now have sealed INBUILT antenna, there's not much possible in the way of external connections to enhance weak signals.

Using a DIY parabolic dish such as this simply concentrates the weak wireless signals onto the antenna sited at the focal point - flexible mounting allows positioning for the best reception.

Conveniently ANY microwave signals come to the same FP - so the design will enhance 900/1800MHz cell phones, 2GHz IPWireless & "b/g" 2.4GHz & even "a" 5.4 GHz WiFi. Tests with PDA utility **WiFiFoFun** indicate 12dB gain readily achieved = 4 times range!

Dell Axim X5 PDA with Socket low power CF WiFi card at focal point (~75mm out) of cheap 320mm diam "parabolic" wok.

This wok 320mm diam & ~85mm depth to centre

Verify focal point position by perhaps bringing the sun's reflection to a point - line the wok with aluminium foil for the trial if it's matt as here.

Of course the parabola formula for FP position can be used too

$$F = \frac{\text{Diam}^2}{16 \times C} \sim \frac{320\text{mm} \times 320\text{mm}}{16 \times 85\text{mm}} \sim 75\text{mm from centre}$$

( C = centre depth )

Cheap compact camera tripod

Floppy disk case makes convenient cradle & allows swap out with cell phones etc too !

Spring paper clip allows secure but quick fit to dish  
Clip bolted to back of cradle - pack out with plastic etc if need be

Respect GSM cell phones have 35km distance limit.

Although hard to talk like this ( unless you've a Blue Tooth headset ) in marginal locations inward text messages at least can get thru' !

Via Stan. SWAN => s.t.swan@massey.ac.nz <= June 2004  
See full "Parabolic Cookware" WiFi details => www.usbwifi.orcon.net.nz



# Homemade Antenna

Refer to USB WiFi resource page  
=> [www.usbwifi.orcon.net.nz](http://www.usbwifi.orcon.net.nz)

October 2004

This aluminium mesh covered "\$2 Shop" kids umbrella yielded ~12dB gain with a WiFi capable PDA (Dell Axim X5 & Socket CF), even though only ~parabolic. Remove fabric to reduce wind resistance of course ! Mesh MUST be uniformly conductive with gaps < .1 wavelength. For 2.4Ghz WiFi this means  $\lambda = 125\text{mm}$ , so .1 wavelength ~12mm (conveniently thus ~ half inch) 2mm mesh gap is thus well within needs!

FP this umbrella ~ 200mm out, - cut handle to suit & give support to USB adaptor or PDA/cell phone

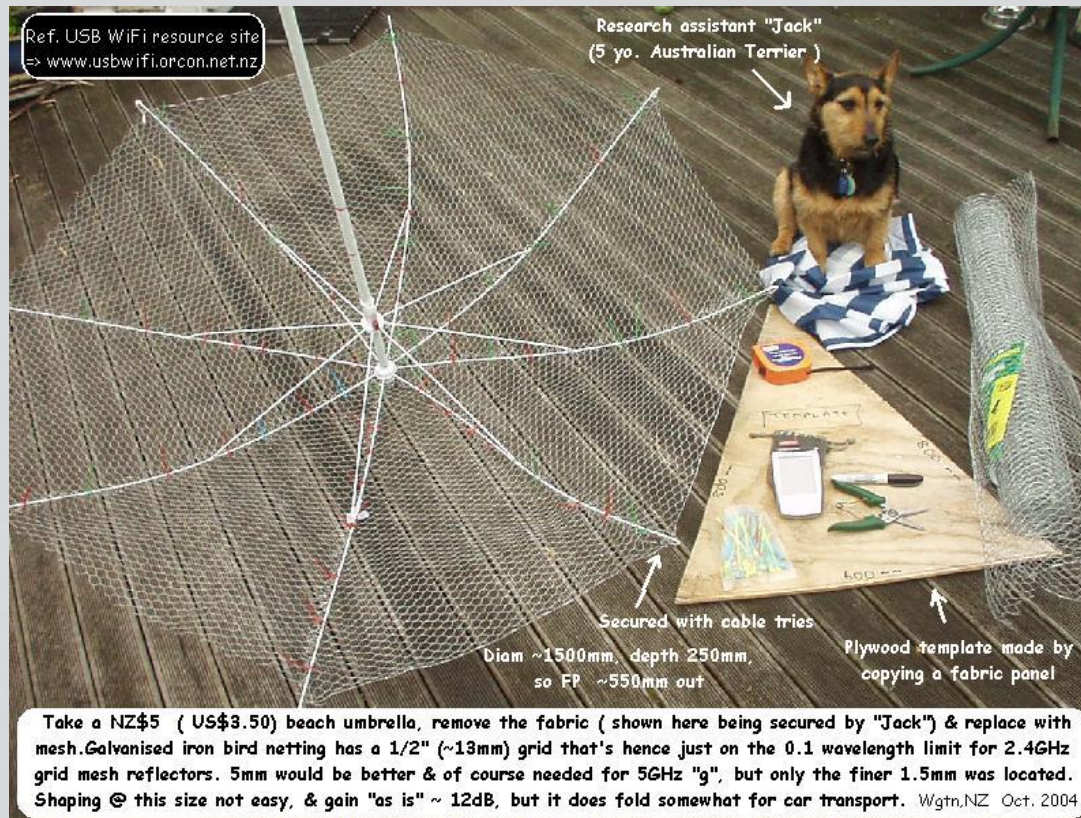
Aluminium 2mm grid fly screen mesh like this is sold by most larger hardware stores, typically 910mm wide, with costs ~ US\$5 /m. Just a modest amount will cover such a frame, & the softer aluminium is gentler to fingers than iron mesh! It cuts easily with snips too. Here it's shown secured both with cable ties & the original (refitted) fabric.

Simple tensioning of supports, perhaps with galvanised iron tie wire or nylon fishing line, could readily improve performance. ~ 18dB ?



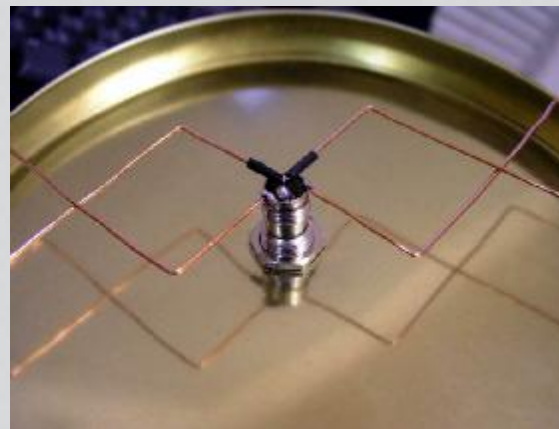


# Homemade Antenna



# Homemade Antenna

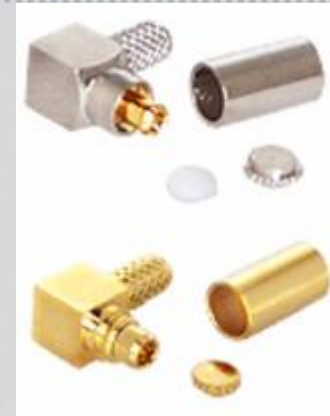
- ❖ Satellite TV Antenna  
+ Hertz Antenna
- ❖ Diamond Dipole  
+ Reflector
- ❖ USB Doggle  
+ Paraboloid
- ❖ Helix Antenna



# Pigtail

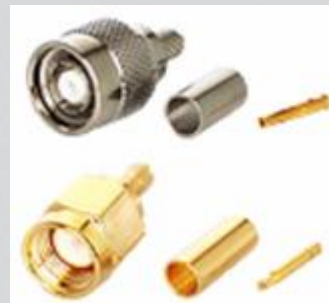
## ◆ Device

- ◆ MC-CARD (Lucent Family)
- ◆ MMCX (Others)



## ◆ Antenna

- ◆ TNC
- ◆ SMA
- ◆ .....



# Pigtail

- ◆ Connector included
  - ◆ Take a equal pigtail
  
- ◆ Connector not included
  - ◆ Modify
    - ◆ Weld with a connector
      - ◆ Nice looking
    - ◆ Weld with a cable
      - ◆ Nice performance



# Example 1

## ◆ Siemens SS2521



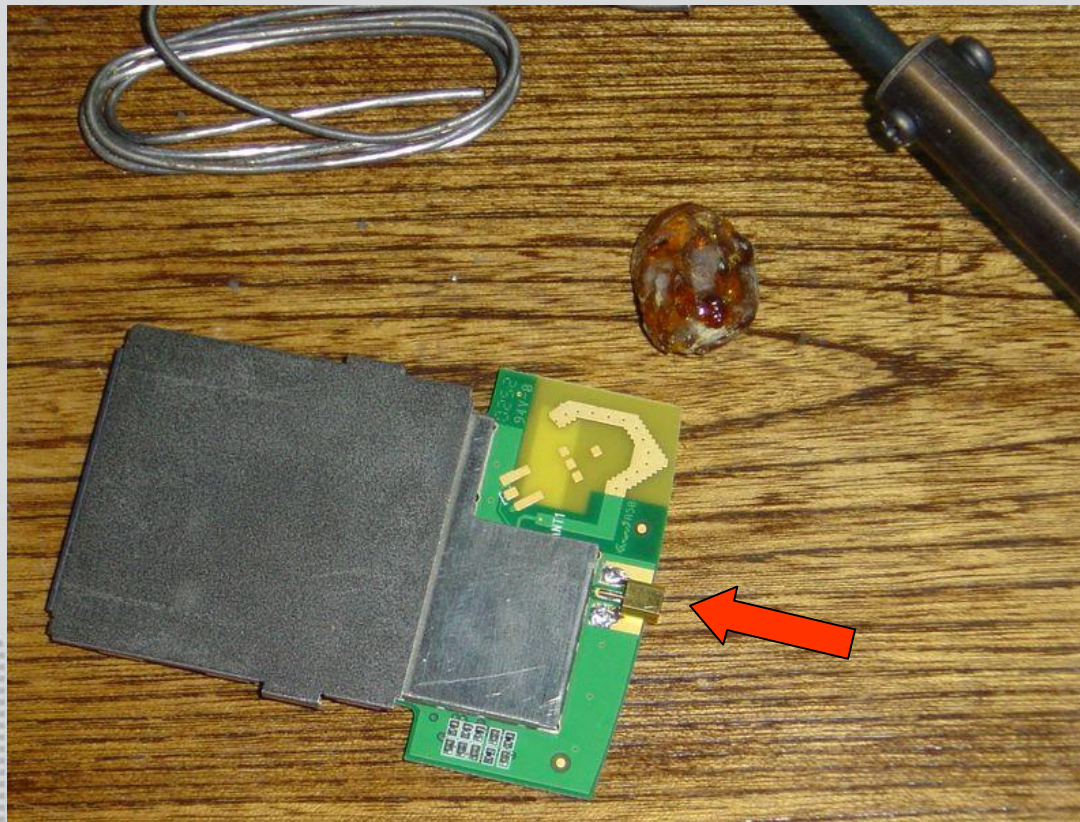
# Example 1

◆ Open



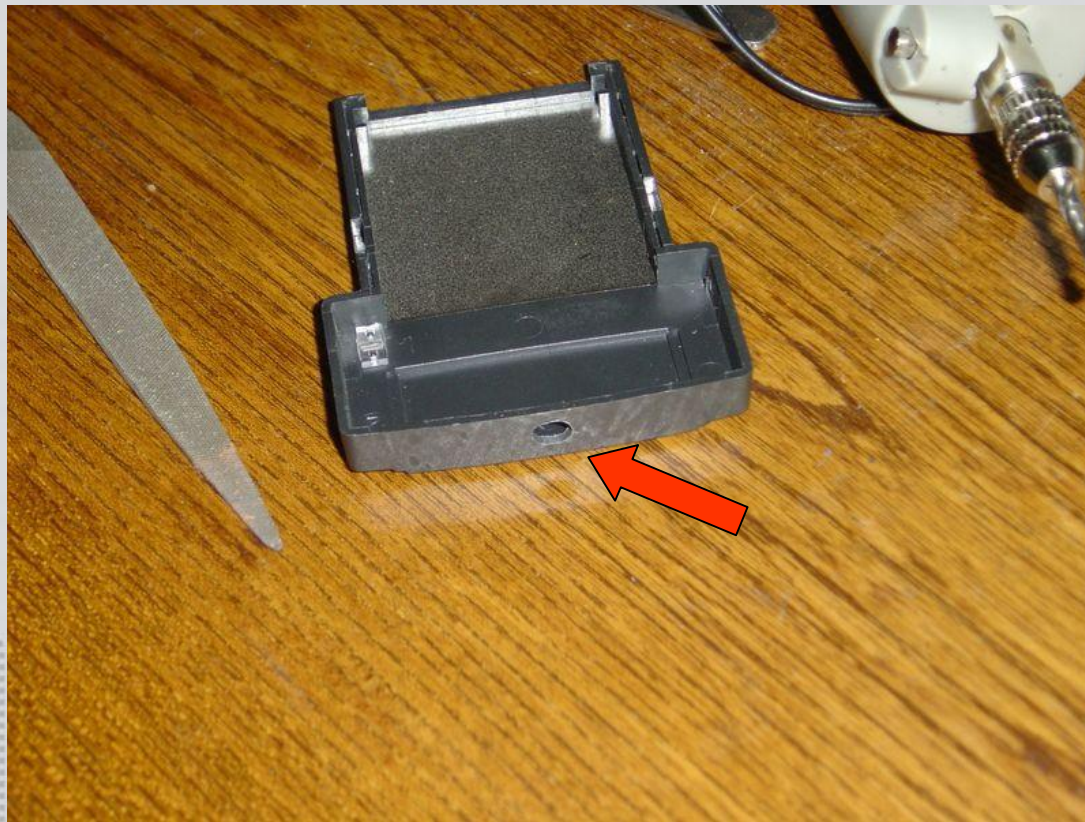
# Example 1

- ✦ Weld a MMCX connector



# Example 1

✦ Drilled the shell





# Example 1

❖ WiFi Card + PDA + Yagi Antenna



# Example 1

Let's work together !



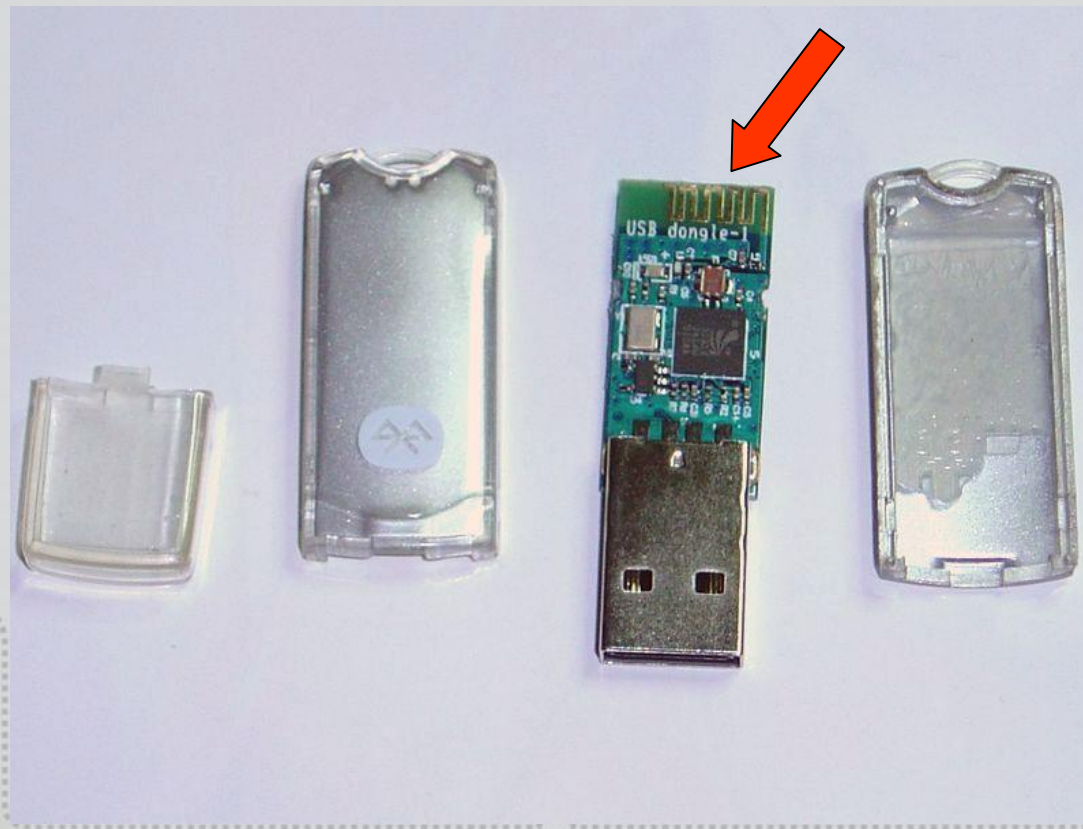
## Example 2

- ◆ A cheap Class 2 bluetooth doggle



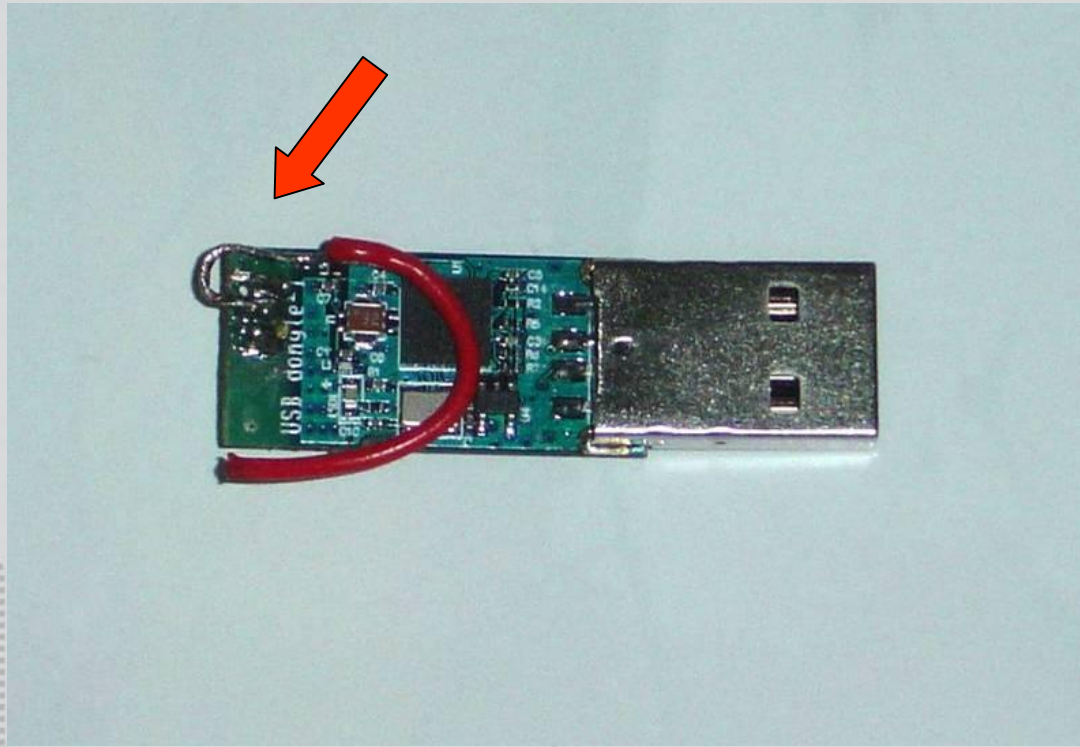
## Example 2

- ◆ Intenerate glue with hair drier



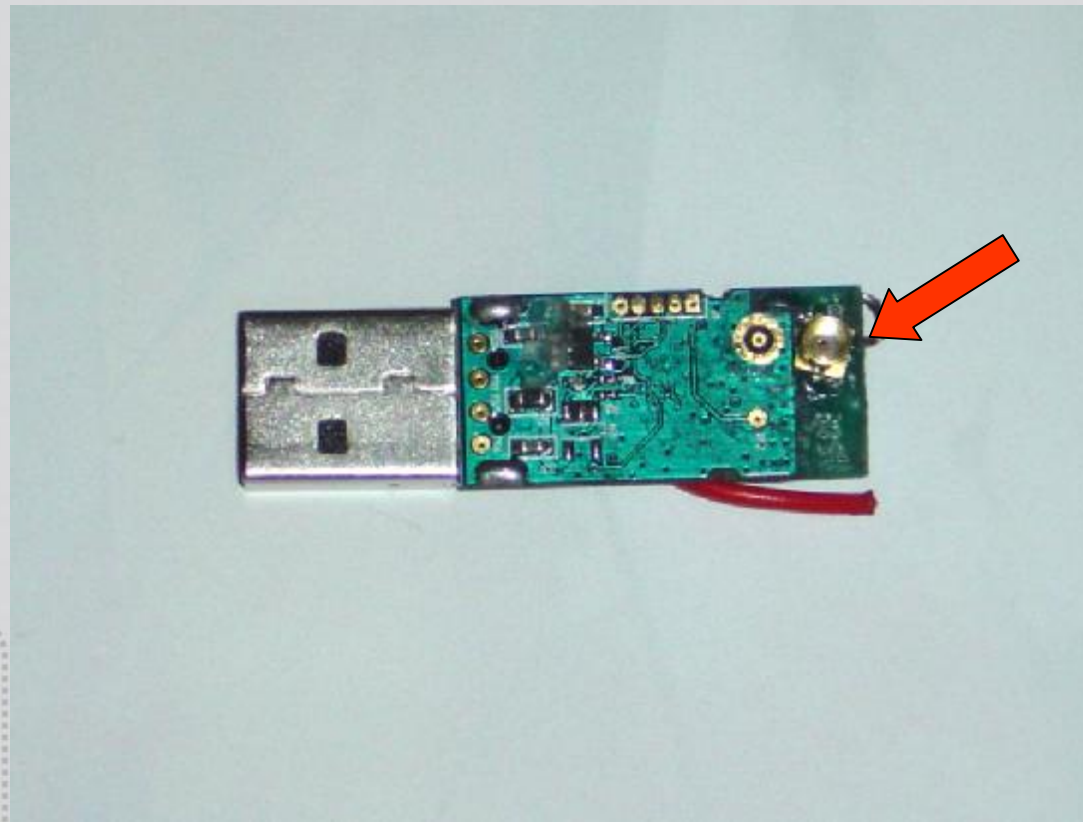
## Example 2

- ✦ Scrape off the print antenna, weld with a short wire



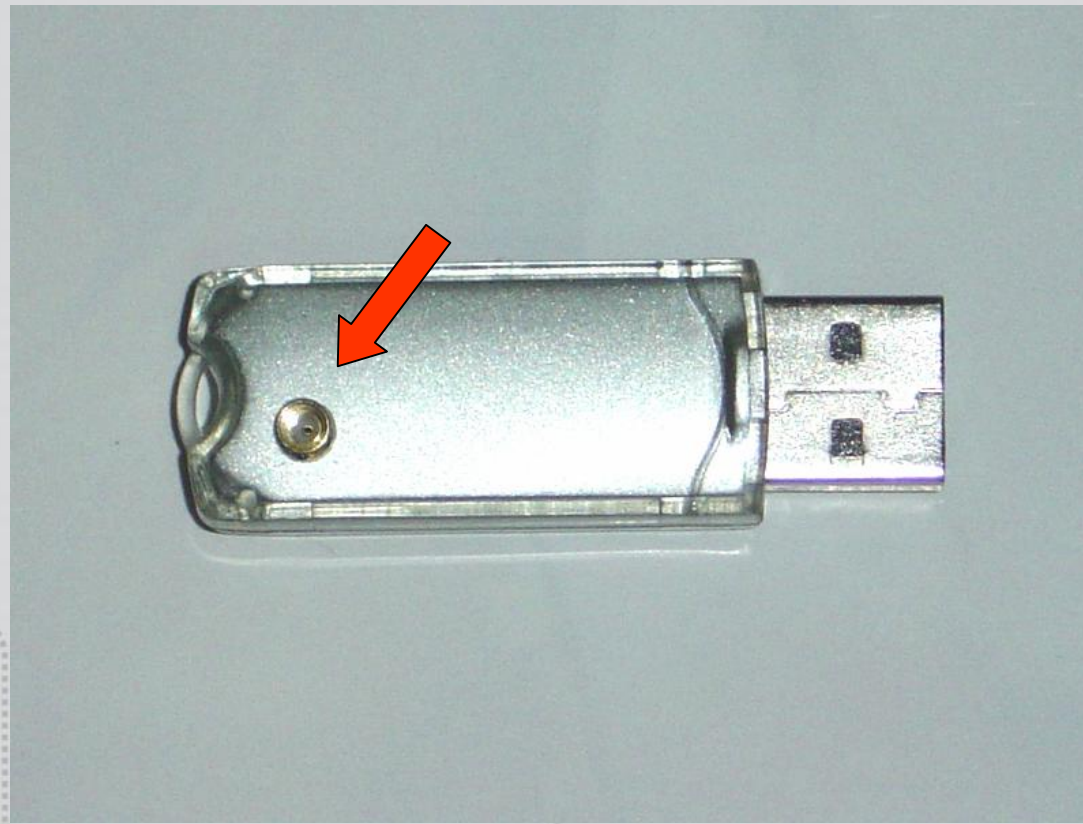
## Example 2

- ✦ Drill PCB for welding MMCX



## Example 2

✦ Drill shell for MMCX



# Example 2

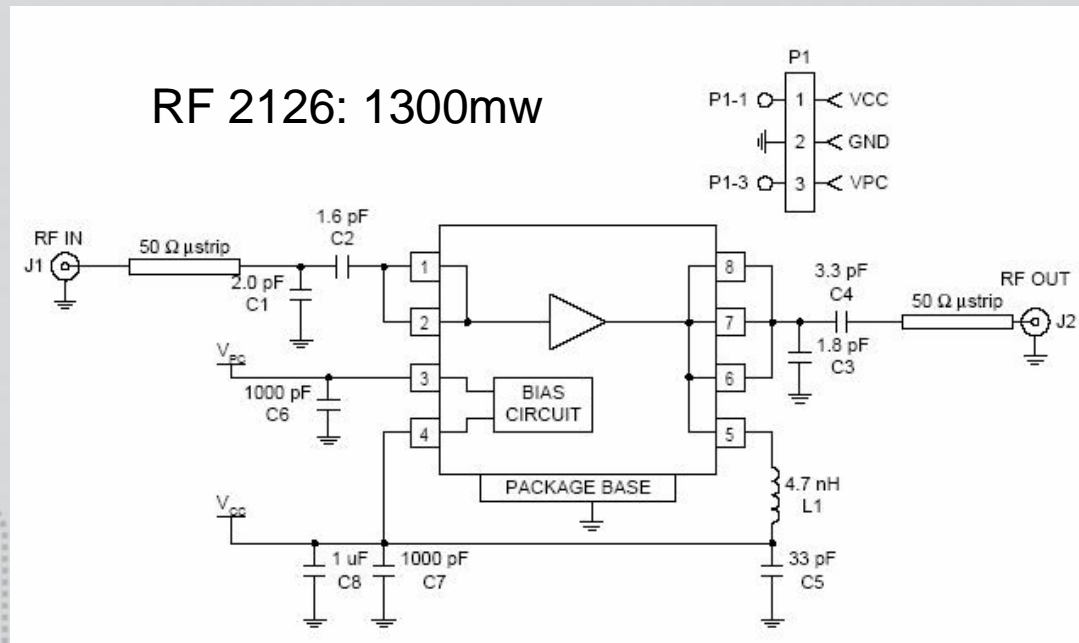
Done !





# What else should we do ?

- ◆ Homemade a RF microwave amplifier
- ◆ More than 1000mw output power



DEFCON

# Wifi Shootout

X'con 2005

- ◆ 2004
  - ◆ 55.1 miles
- ◆ 2005
  - ◆ 125 miles
- ◆ 2006
  - ◆ ?



XFOCUS TEAM

BEIJING.CHINA

2002-2005



See you next year  
See you XCon 2006 !

• tombkeeper[0x40]xfocus.org •



X'con 2005