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

Chose your wifi card

- Chipset & Compatibility
  - Support monitor/master mode ?
  - Support packet injection?
  - Support linux ?
    - Ndiswapper 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	-90 dBm
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

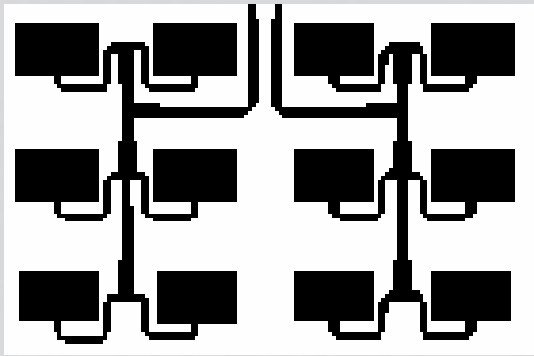
- Yagi Antenna
  - 10 dBi ~ 16 dBi
- "Flat Panel Antenna #
  - 5 dBi ~ 24 dBi
- Homemade Antenna
  - Good pastime
  - No bad gain

Yagi Antenna

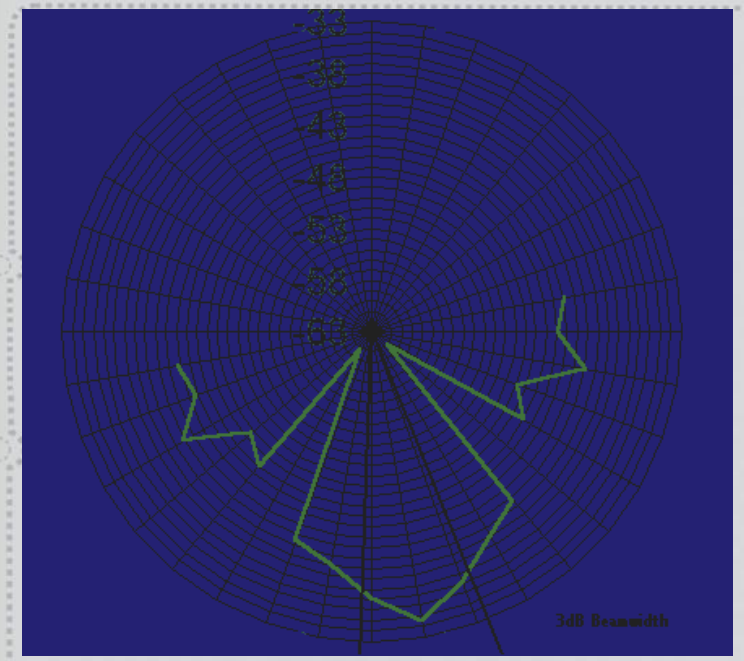
- Hidetsugu Yagi & Shintaro Uc
- Cheap price
  Acceptable size
- Medium gain

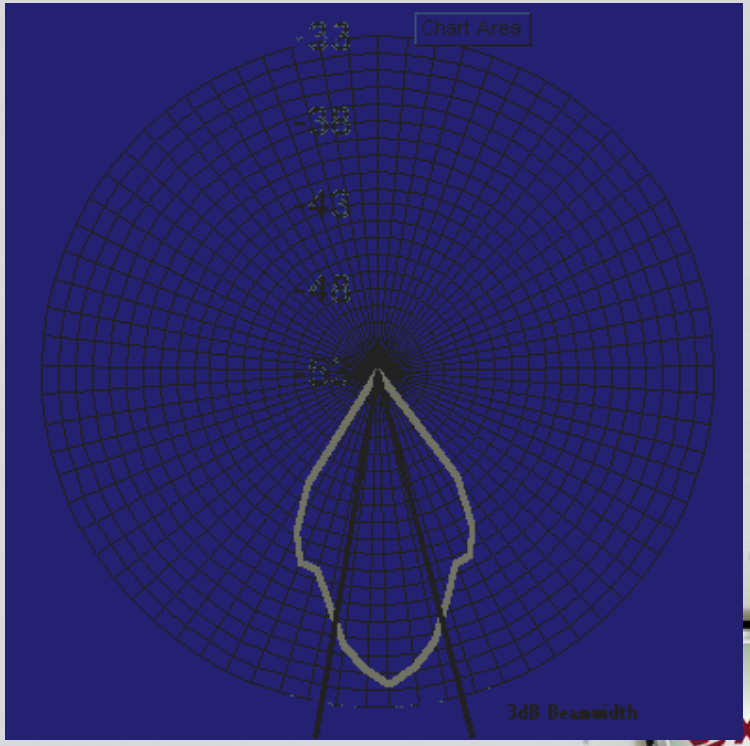
!Flat Panel Antenna"

- Could more than 20dBi
- Portable
- Maybe expensive



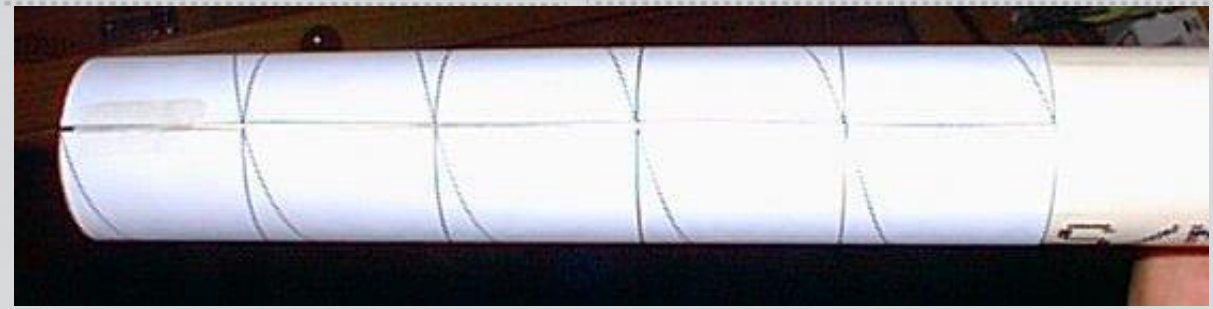
Homemade Antenna

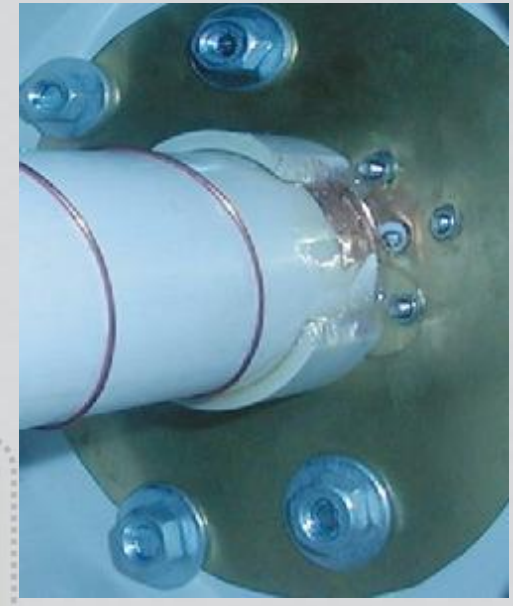


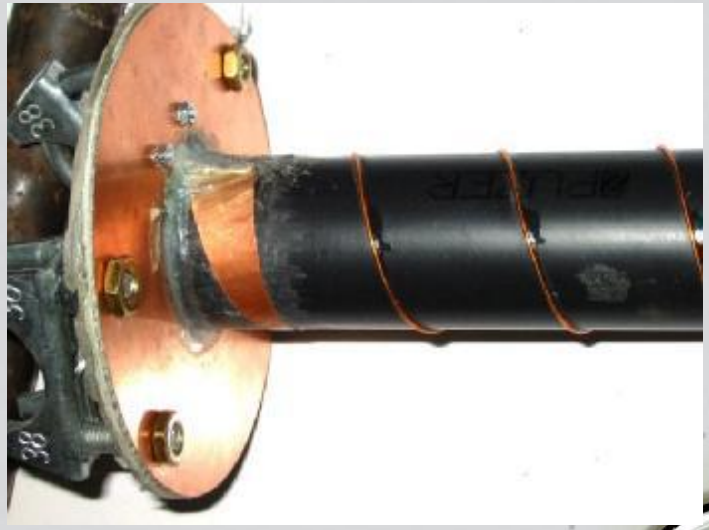


Homemade Antenna

Homemade Antenna







Homemade Antenna

Homemade Antenna

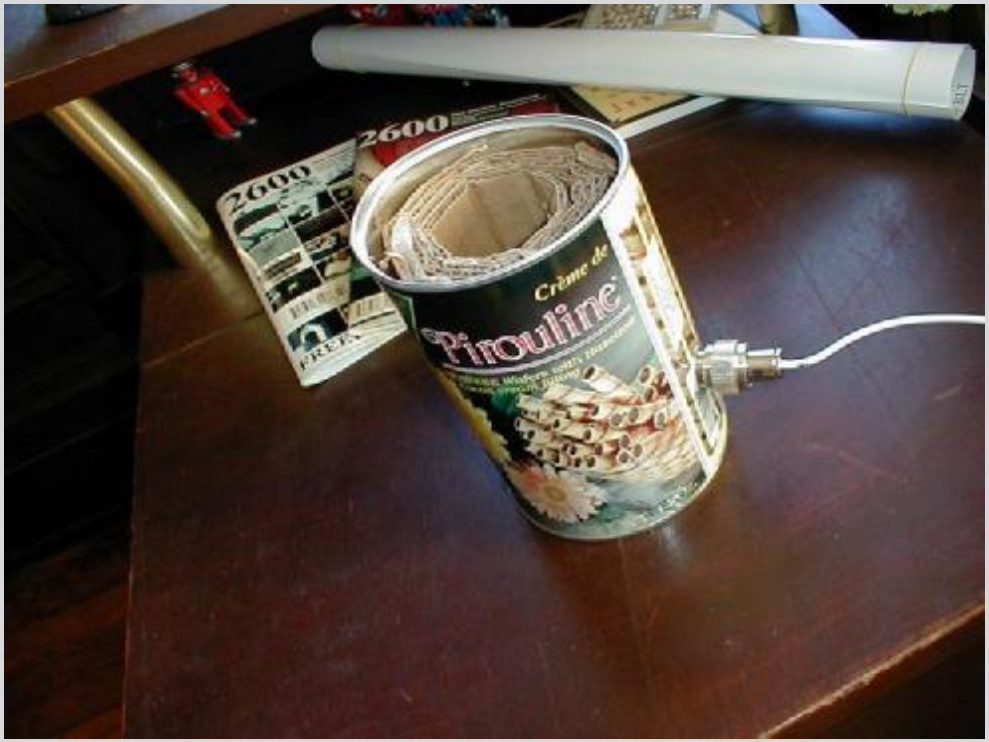
Homemade Antenna

Homemade Antenna

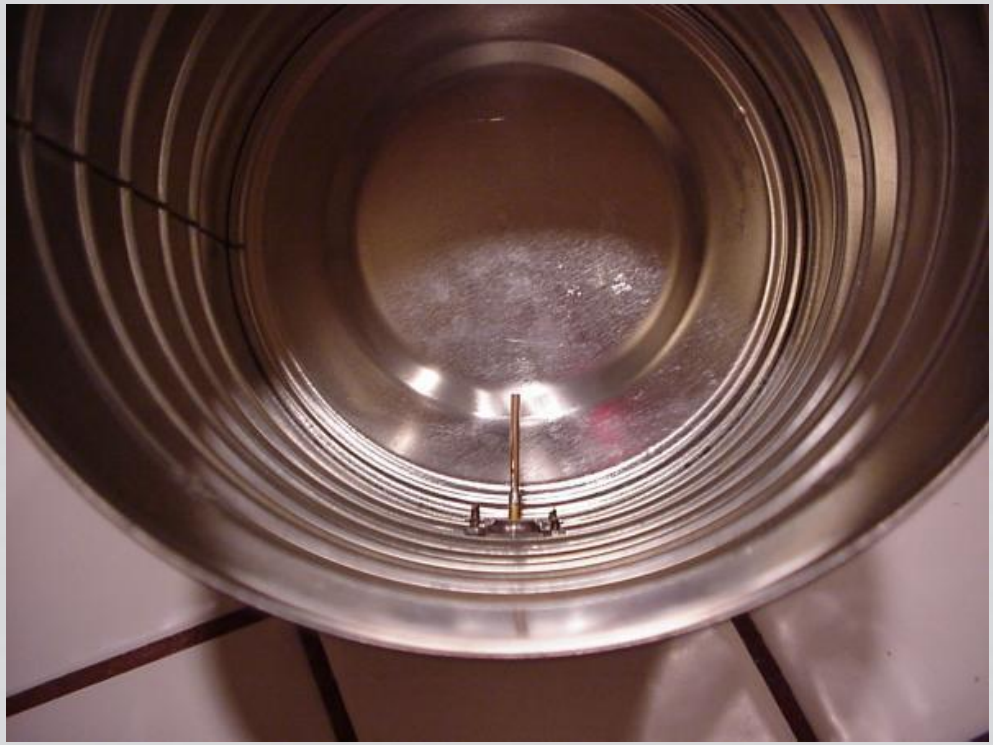
Homemade Antenna

Homemade Antenna

Homemade Antenna



Homemade Antenna



Homemade Antenna

Homemade Antenna

Homemade Antenna

Homemade Antenna