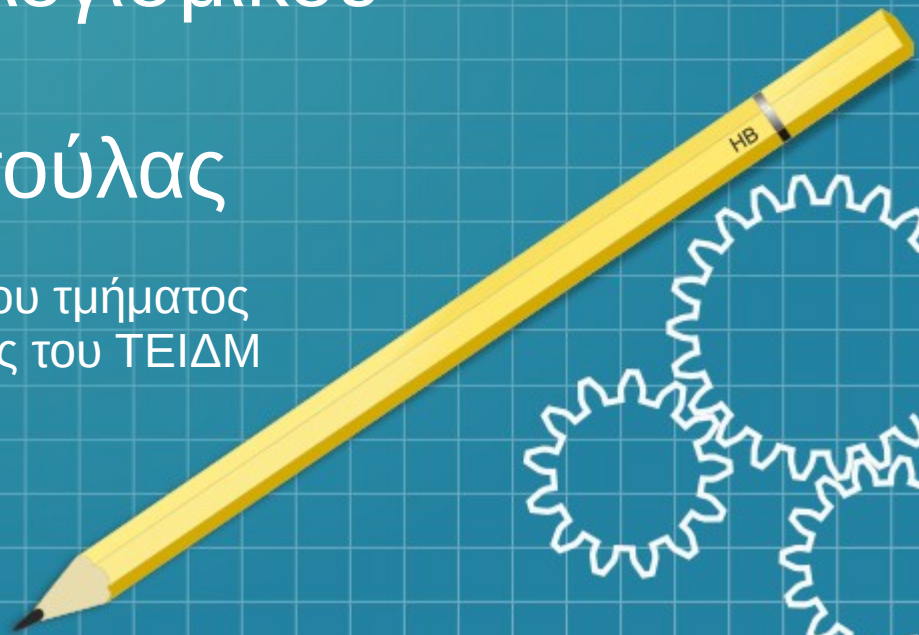
“RF Hacking”

Γνωριμία με τον κόσμο των Ραδιοσυχνοτήτων
και του ανοιχτού λογισμικού

Δημήτριος Ντούλας

Προπτυχιακός φοιτητής του τμήματος
Μηχανικών Πληροφορικής του ΤΕΙΔΜ



Τί είναι το RF Hacking;

- **RF** = Radio Frequency
- Ο **ραδιοερασιτεχνισμός** είναι μια υπηρεσία ραδιοεπικοινωνίας, που έχει ως σκοπό την αυτοδιδασκαλία, την αλληλοεπικοινωνία, την **τεχνολογική έρευνα** των ραδιοερασιτεχνών καθώς και την τηλεπικοινωνιακή υποστήριξη επιχειρήσεων βοηθείας σε περιπτώσεις καταστάσεων έκτακτης ανάγκης και καταστροφών. Η υπηρεσία αυτή διεξάγεται από ραδιοερασιτέχνες, οι οποίοι ασχολούνται με τη ραδιοηλεκτρική τεχνική αποκλειστικά για προσωπικό σκοπό χωρίς όφελος.

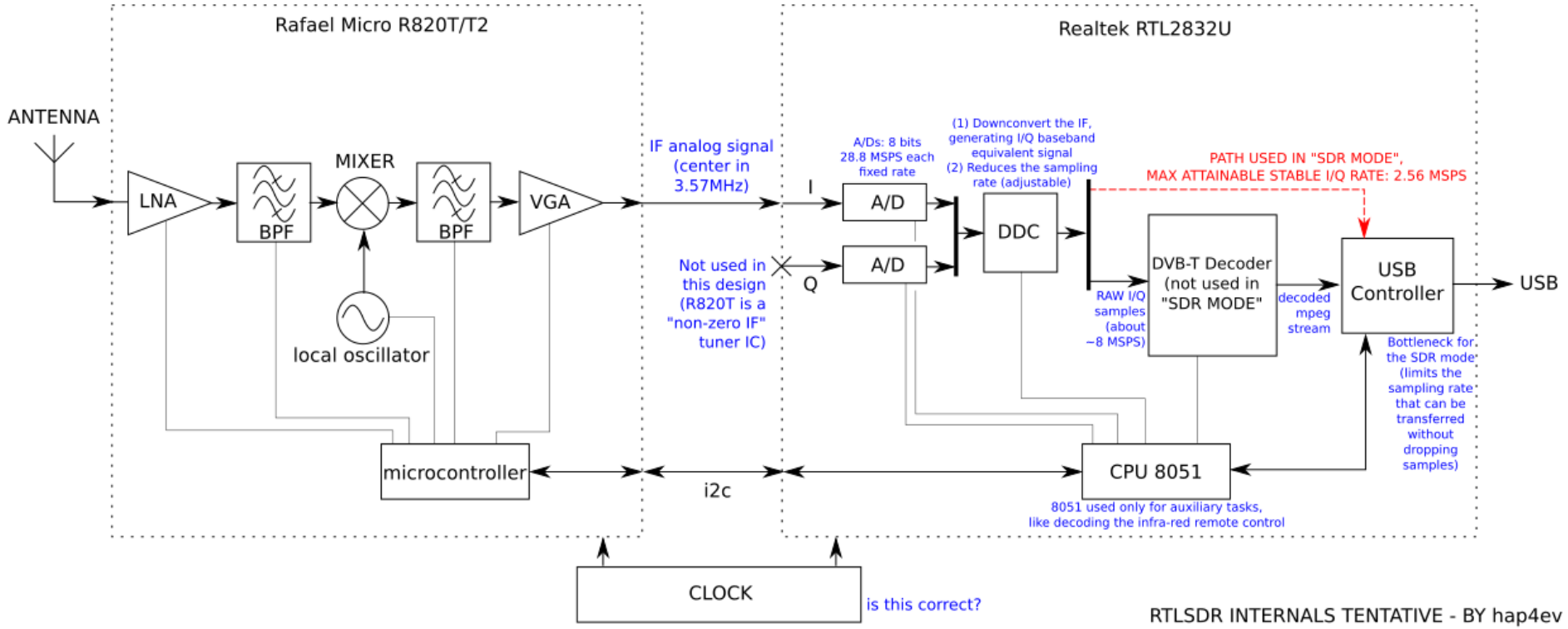
  Προκειμένου να γίνει κανείς ραδιοερασιτέχνης είναι απαραίτητο α) να αποκτήσει πτυχίο ραδιοερασιτέχνη και β) να του χορηγηθεί άδεια ερασιτεχνικού σταθμού ασυρμάτου
- **Hacking** = Η εκμάθηση της λειτουργίας ενός συστήματος σε βάθος και ο **αυτοσχεδιασμός** στη χρήση του.

Πως ξεκίνησαν όλα για το RTL-SDR

- Τα πρώτα βήματα έγιναν από τον Eric Fry που το 2010 έκανε κάποιες δοκιμές προσπαθώντας να κάνει ένα DVB TV tuner να παίξει στο Linux.
- Κατόπιν ο Antti Palosaari έγραψε ένα εναλλακτικό οδηγό (driver) όπου το TV Tuner θα εμφανιζότανε ως SDR.
- Ο οδηγός αυτός παρέκαμπτε το κύκλωμα αποδιαμόρφωσης και μπορούσε να πάρει κατευθείαν την RAW δειγματοληψία του δέκτη.

To RTL-SDR

Λειτουργία

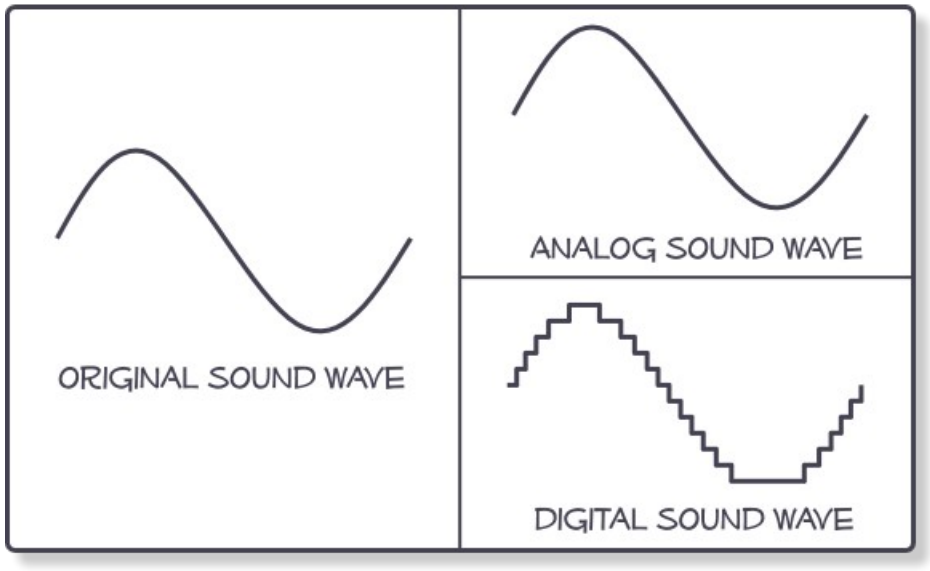

Rafael Micro R820T/T2
Realtek RTL2832U
ANTENNA
LNA
BPF
MIXER
BPF
VGA
local oscillator
IF analog signal (center in 3.57MHz)
Not used in this design (R820T is a "non-zero IF" tuner IC)
I
Q
A/D
A/D
A/Ds: 8 bits 28.8 MSPS each fixed rate
(1) Downconvert the IF, generating I/Q baseband equivalent signal (2) Reduces the sampling rate (adjustable)
DDC
PATH USED IN "SDR MODE", MAX ATTAINABLE STABLE I/Q RATE: 2.56 MSPS
RAW I/Q samples (about ~8 MSPS)
DVB-T Decoder (not used in "SDR MODE"
decoded mpeg stream
USB Controller
USB
Bottleneck for the SDR mode (limits the sampling rate that can be transferred without dropping samples)
microcontroller
i2c
CPU 8051
8051 used only for auxiliary tasks, like decoding the infra-red remote control
CLOCK
is this correct?
RTLSDR INTERNALS TENTATIVE - BY hap4ev

Χαρακτηριστικά του Realtek RTL2832U

- outputs 8-bit I/Q-samples
- sample-rate is 3.2 MS/s
- frequency range
  - Elonics E4000

    52 - 2200 MHz
  - Rafael Micro R820T

    24 - 1766 MHz



Άλλα SDR

Comparisons with other common Wideband Commercial Software Defined Radios

SDR	Tune Low (MHz)	Tune Max (MHz)	RX Bandwidth (MHz)	ADC Resolution (Bits)	Transmit? (Yes/No)	Price ($USD)
RTL-SDR (R820T)	24	1766	3.2	8	No	~20
Funcube Pro+	0.15 410	260 2050	0.192	16	No	~200
Airspy	24	1800	10	12	No	199
SDRPlay	0.1	2000	8	12	No	149
HackRF	30	6000	20	8	Yes	299
BladeRF	300	3800	40	12	Yes	400 & 650
USRP 1	DC	6000	64	12	Yes	700

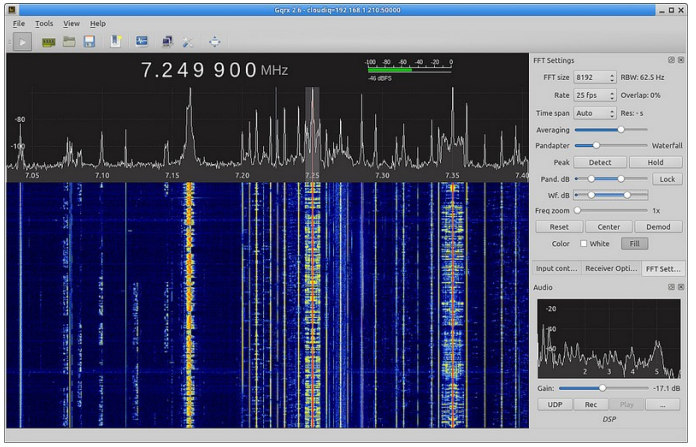
Τι καλύπτει σε συχνότητες

- Use as a police radio scanner.
- Listening to EMS/Ambulance/Fire communications.
- Listening to aircraft traffic control conversations.
- Tracking aircraft positions like a radar with ADSB decoding.
- Decoding aircraft ACARS short messages.
- Scanning trunking radio conversations.
- Decoding unencrypted digital voice transmissions such as P25/DMR/D-STAR.
- Tracking maritime boat positions like a radar with AIS decoding.
- Decoding POCSAG/FLEX pager traffic.
- Scanning for cordless phones and baby monitors.
- Tracking and receiving meteorological agency launched weather balloon data.
- Tracking your own self launched high altitude balloon for payload recovery.
- Receiving wireless temperature sensors and wireless power meter sensors.
- Listening to amateur radio and CB.
- Decoding ham radio APRS packets.
- Watching analogue broadcast TV.
- Sniffing GSM signals.
- Using rtl-sdr on your Android device as a portable radio scanner.
- Receiving GPS signals and decoding them.
- Using rtl-sdr as a spectrum analyzer.
- Receiving NOAA weather satellite images.
- Listening to satellites.
- Radio astronomy.
- Monitoring meteor scatter.
- Listening to FM radio, and decoding RDS information.
- Listening to DAB broadcast radio.
- Listening to and decoding HD-Radio (NRSC5).
- Use rtl-sdr as a panadapter for your traditional hardware radio
- Use rtl-sdr as a high quality entropy source for random number generation.
- Use rtl-sdr as a noise figure indicator.
- Reverse engineering unknown protocols.
- Triangulating the source of a signal.
- Searching for RF noise sources.
- Characterizing RF filters
- Listening to the ISS (International Space Station).
-
- Furthermore, with an upconverter or V3 RTL-SDR dongle to receive HF signals the applications are expanded to:
-
- Listening to amateur radio hams on SSB with LSB/USB modulation.
- Decoding digital amateur radio ham communications such as CW/PSK/RTTY/SSTV.
- Receiving HF weatherfax.
- Receiving digital radio mondiale shortwave radio (DRM).
- Listening to international shortwave radio.
- Looking for RADAR signals like over the horizon (OTH) radar, and HAARP signals.

Λογισμικό open source

- Librtlsdr
  - rtl_sdr
  - rtl_tcp
  - rtl_fm
- rtl_fm -f 96.3e6 -M wbfm -s 200000 -r 48000 - | aplay -r 48k -f S16_LE

- GNU Radio
  - GRC
  - GQRX



Διαμόρφωση Σημάτων

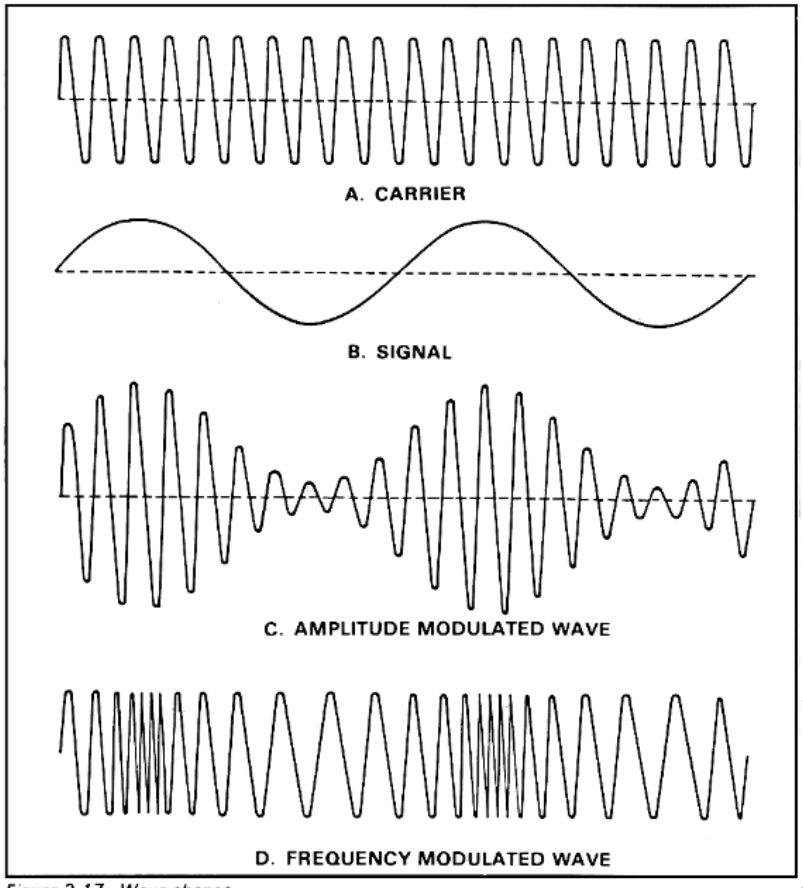
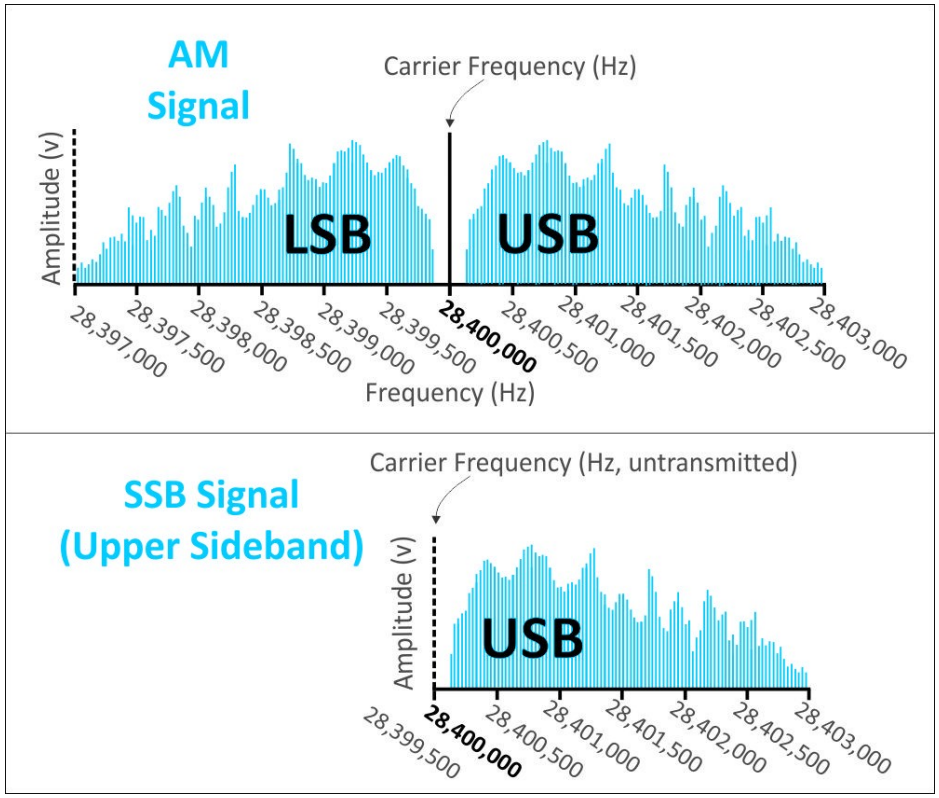
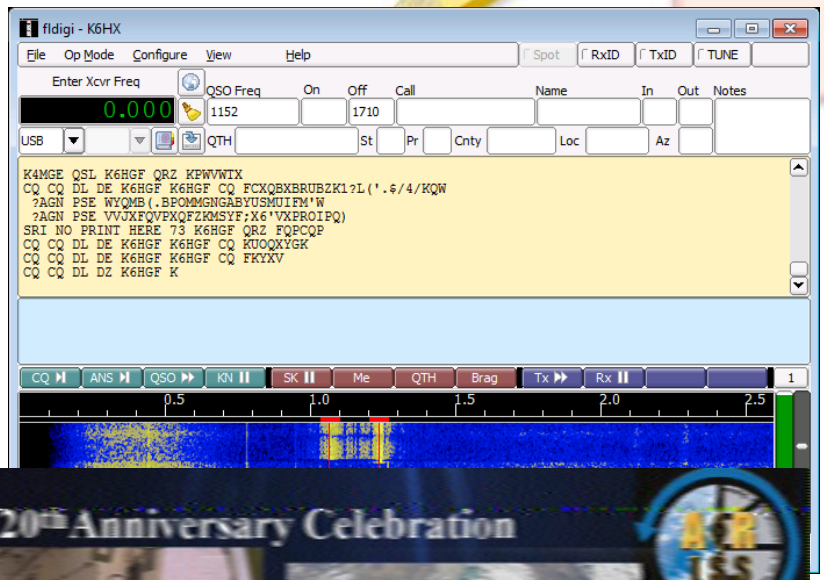


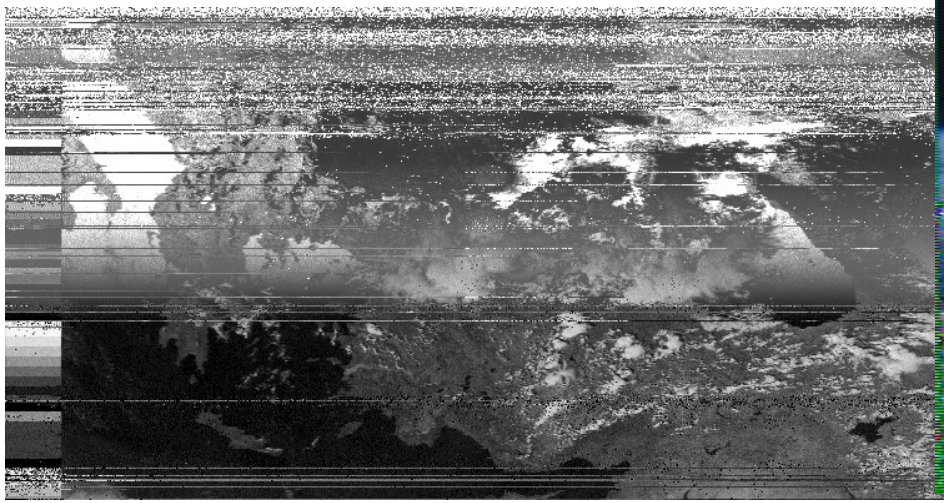
Figure 2-17. Wave shapes.



Αποκωδικοποίηση σημάτων

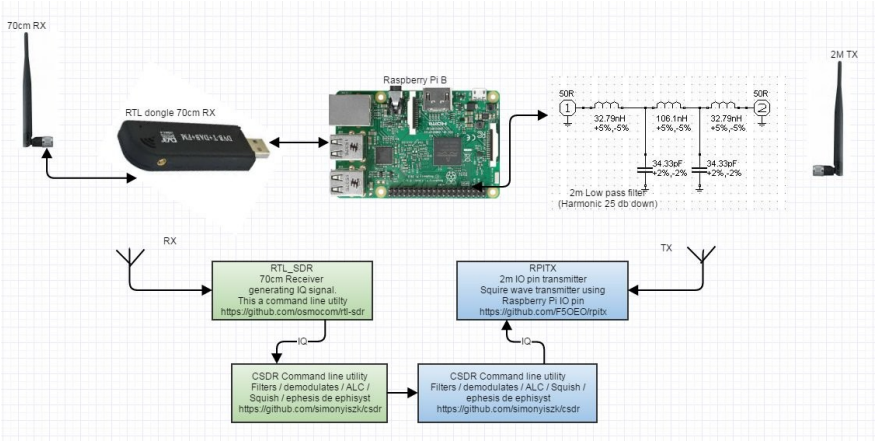
- CW, DTMF
- SSTV, Weather Fax, NOAA APT
- RTTY, FSK, PSK

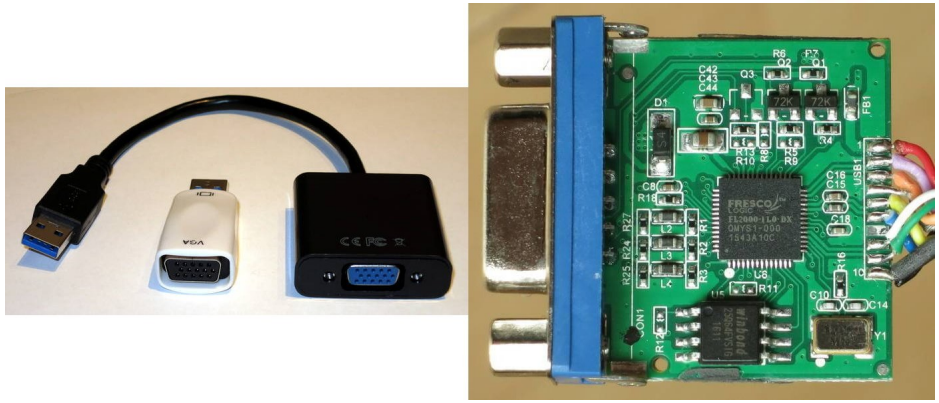




Κατασκευές

Άλλα TX projects





- Raspberry Pi (rpitx)
- USB to VGA adapter (osmo-fl2k)

Προσοχή! Απαιτείται άδεια για εκπομπή.

Ευχαριστώ
73 DE SV2RCK

Ερωτήσεις ;

Email: ntoulasd@yahoo.gr