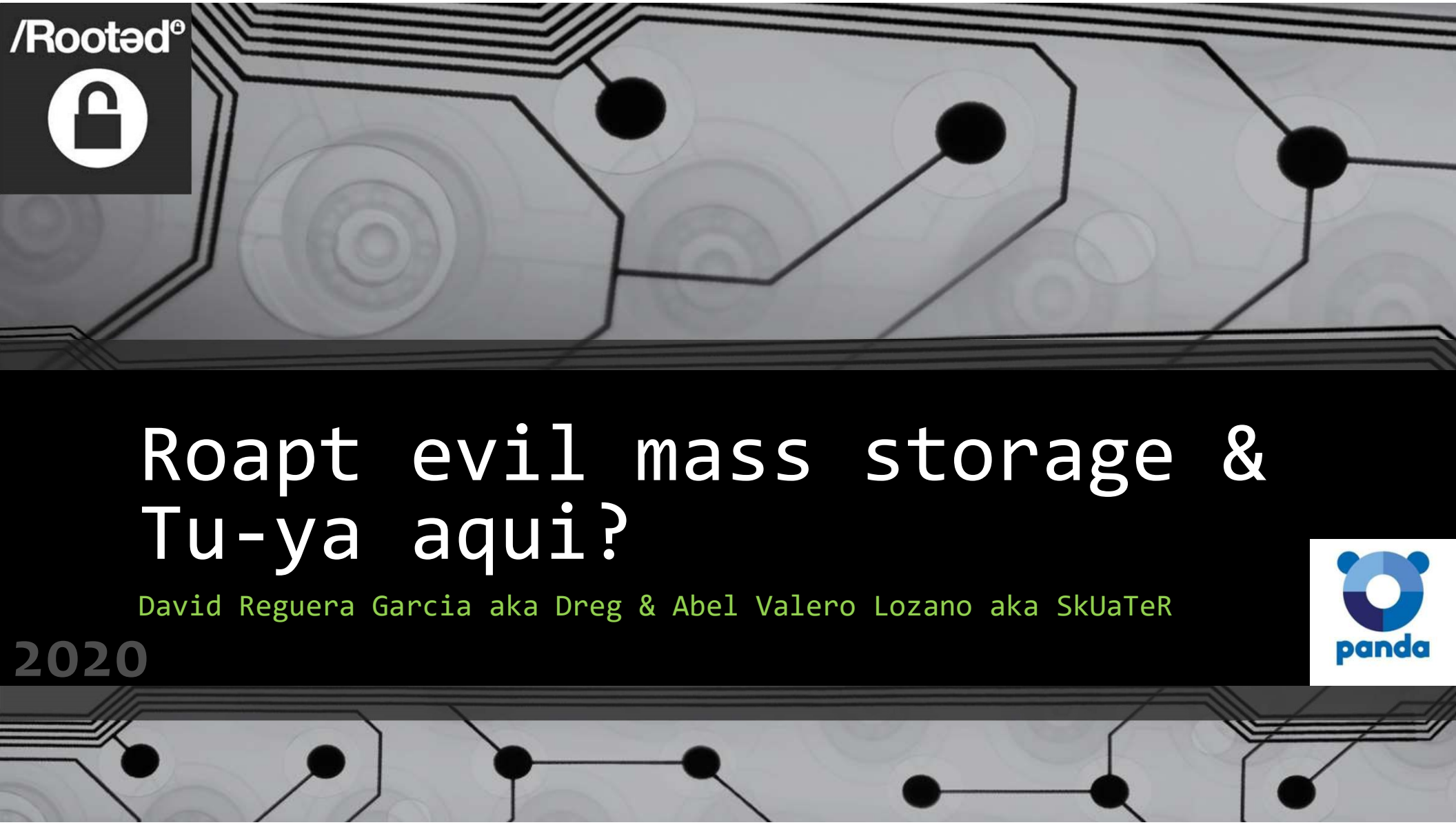


Roapt evil mass storage & Tu-ya aqui?

David Reguera Garcia aka Dreg & Abel Valero Lozano aka SkUaTeR

2020

David Reguera Garcia aka Dreg

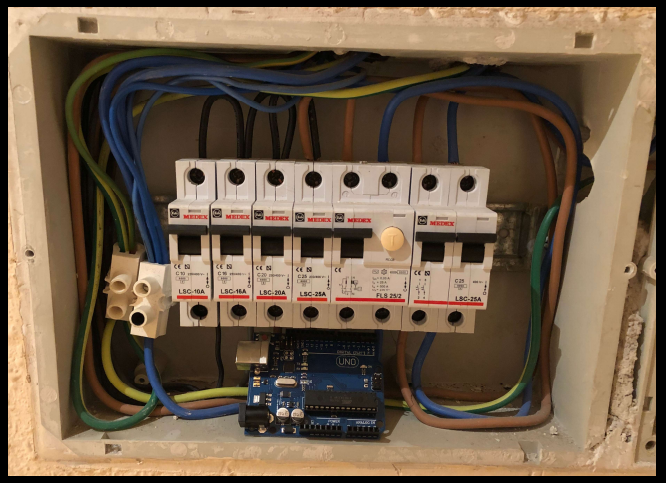
- Senior malware researcher, C, C++, ASM, x86_64, ARM Cortex & AVR-8-bit
- Contributing to rootkit unhooker, unhide, x64dbg, enyelkm, anticuckoo, dbgchild....
- https://github.com/David-Reguera-Garcia-Dreg
- https://twitter.com/fr33project
- http://www.fr33project.org/
- dreg@fr33project.org

evil mass storage – POC just for fun

- infect a **target** machine without NET & exfiltrate info
- hardware: at90usb1287 + atmega328p + ts3usb221 + mosfet + sd card reader (SPI) + rf 433MHz ASK …
- multi-stage malware: only visible when connected to **target**
- exfiltrate info via two ways:
  - mass storage: crypt & hidden sectors
  - radio: rf 433MHz ASK
- firmware: keyboard + mass storage (USB composite device). LUFA + FatFs + Dreg adaptation “USB Mass storage SD card for Teensy2/ATMEGA32U4 by Mathieu Sonet”
- dynamic: serial, VID, PID, USB Descriptor, decrypt/delete sectors…

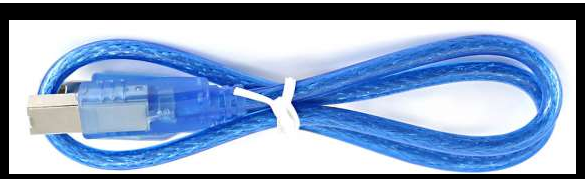
external hardware - receiving data

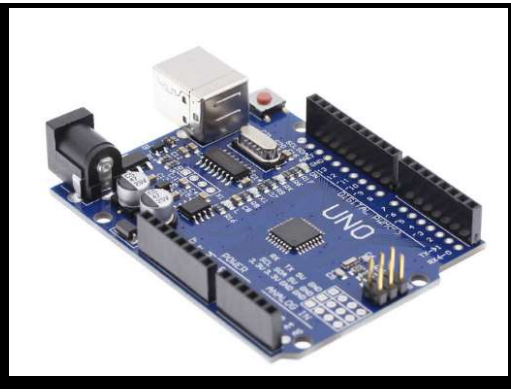
- rf 433mhz receiver
- WIFI AP/STA
- SMS
- GSM/GPRS
- MICRO SD CARD

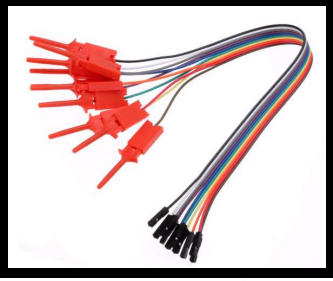


demo prototype

evil mass storage

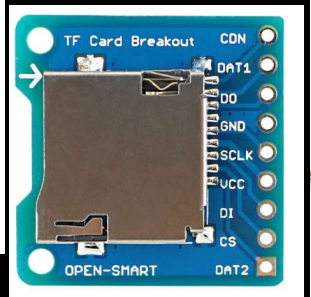


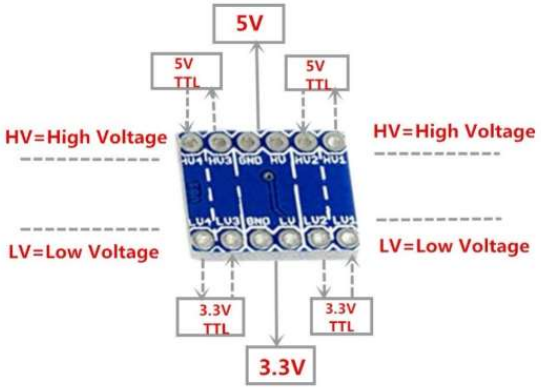


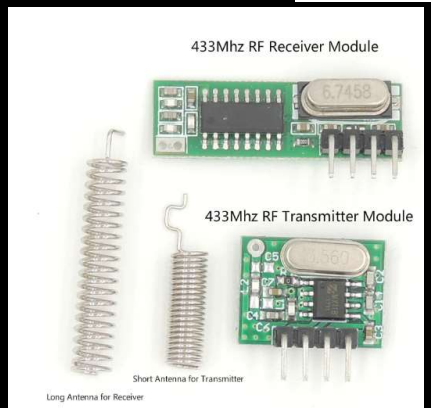


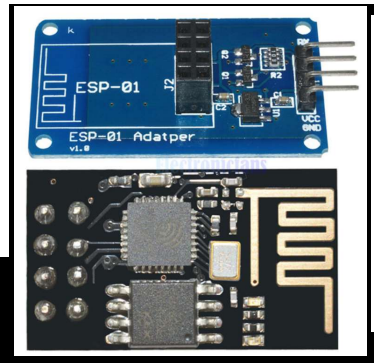
AT90USBKEY

Part Number: AT90USBKEY2



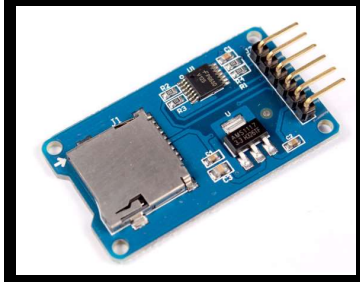


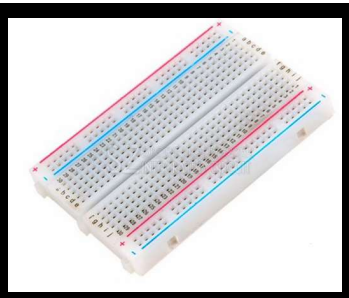



ESP-01
ESP-01 Adatper

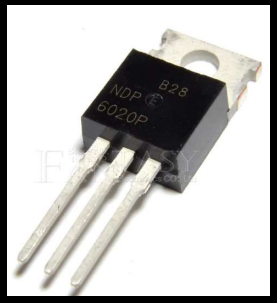

LED INDICATOR
All in one


1000mAh
1000mAh

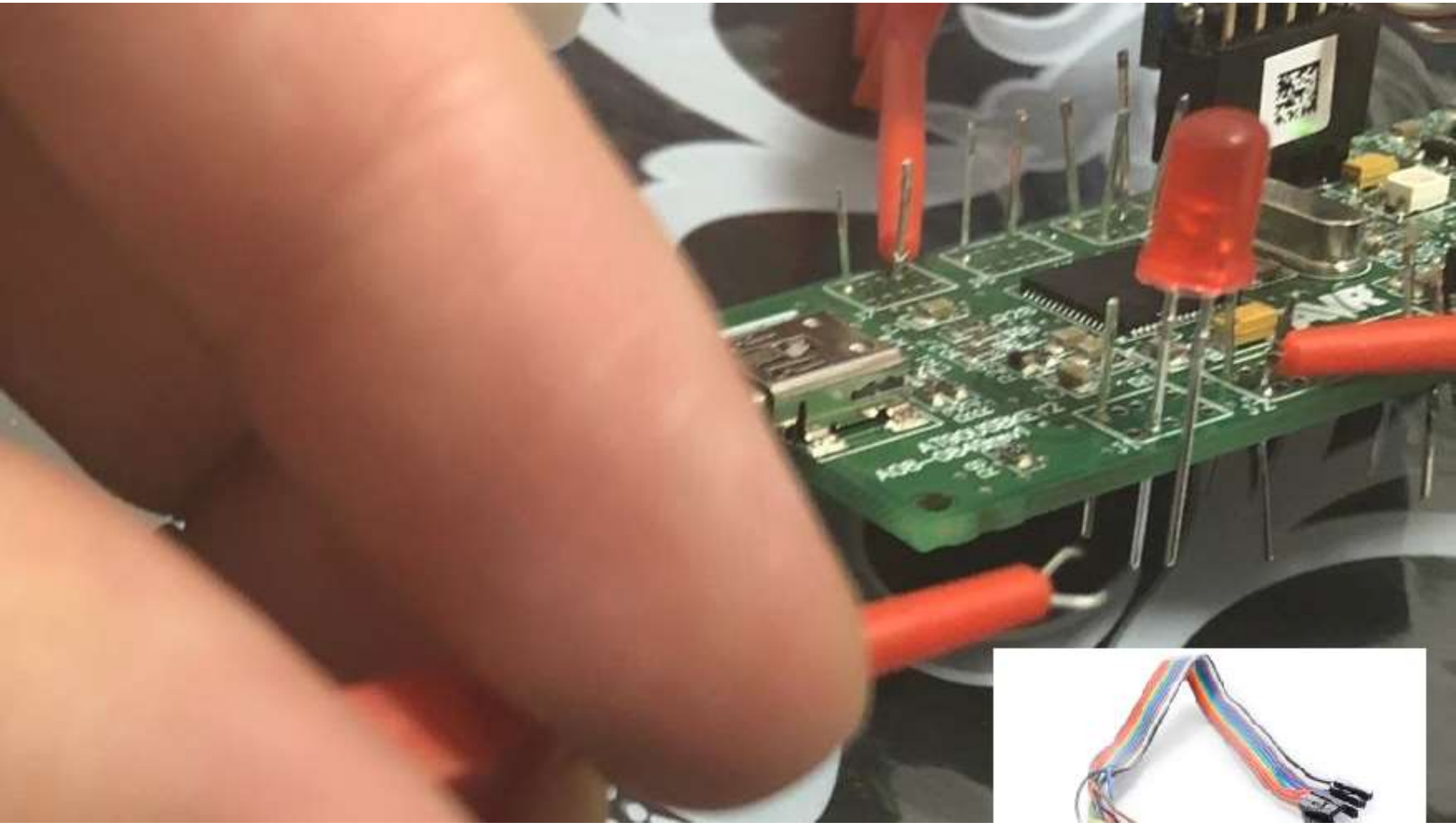





Solder Iron Tip Cleaning Sponge Pad


B28
NDP
6020P


MADE IN CHINA
MEGA 2560



prototype shopping list 1

- mini soldering iron + iron tip
- arduino uno + cable
- arduino mega 2560 + cable
- USB 2.0 Type A 1-Male 1-Female to 5P Screw with/ Shield Terminal Plug Adapter Connector
- USB to DIP Type A 2-Female 1-Male USB Adapter Converter for 2.54mm PCB Board DIY
- ESP-01S ESP8266 Serial Wi-Fi Wireless Module + ESP-01 Adapter for Arduino (5v)
- 400 Tie Points Solderless PCB Breadboard Mini Universal Test Protoboard DIY Bread Board Bus (x2)

prototype shopping list 2

- 4 Channel 5V 3.3V IIC UART SPI TTL Logic Level Converter level conversion module
- 10pcs High Efficiency Test Hook Clip Logic Analyzer Cable Gripper Probe Test Clamp Kit
- kit LEDs 5mm Red Blue Green Yellow White
- mosfet NDP6020P TO-220 NDP6020 TO220 6020P P-channel
- 433 Mhz RF Receiver and Transmitter Module. RX470-4, WL102-341, Short antenna for Transmitter. Long antenna for Receiver
- common values resistor Kit
- DIY TS3USB221 High-Speed USB 2.0 (480Mbps) 1:2 Multiplexer To Demultiplexer Switch With Single Enable Board Module

prototype shopping list 3

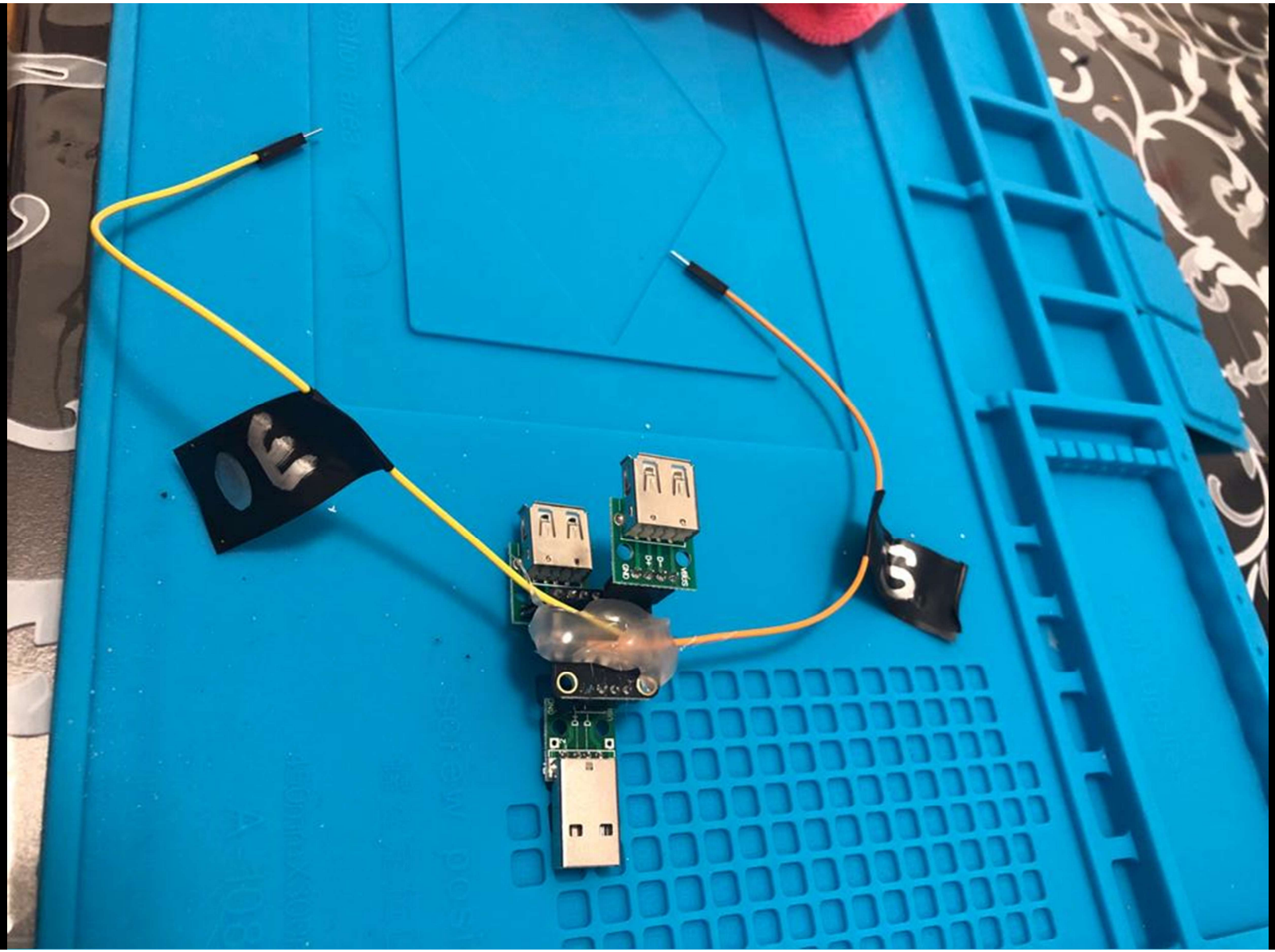
- Reader Adapter for Micro SD USB 2.0 TF M2 MMC MS PRO DUO Card Reader
- 2PCS 9V rechargeable battery large capacity 1000mAh lithium ion rechargeable battery + 1PCS smart 9 V charger
- 9V PP3 Battery Holder Box Case Wire Lead ON/OFF Switch Cover with DC 2.1mm Plug
- SanDisk micro SD card 16GB SDHC + adapter
- DC 9V1A 9V 1A Power Supply AC 100V-240V Converter Adapter Plug Charger 5.5mm x 2.1mm 1000mA
- SIM808 module GSM GPRS GPS Development Board IPX SMA with GPS Antenna

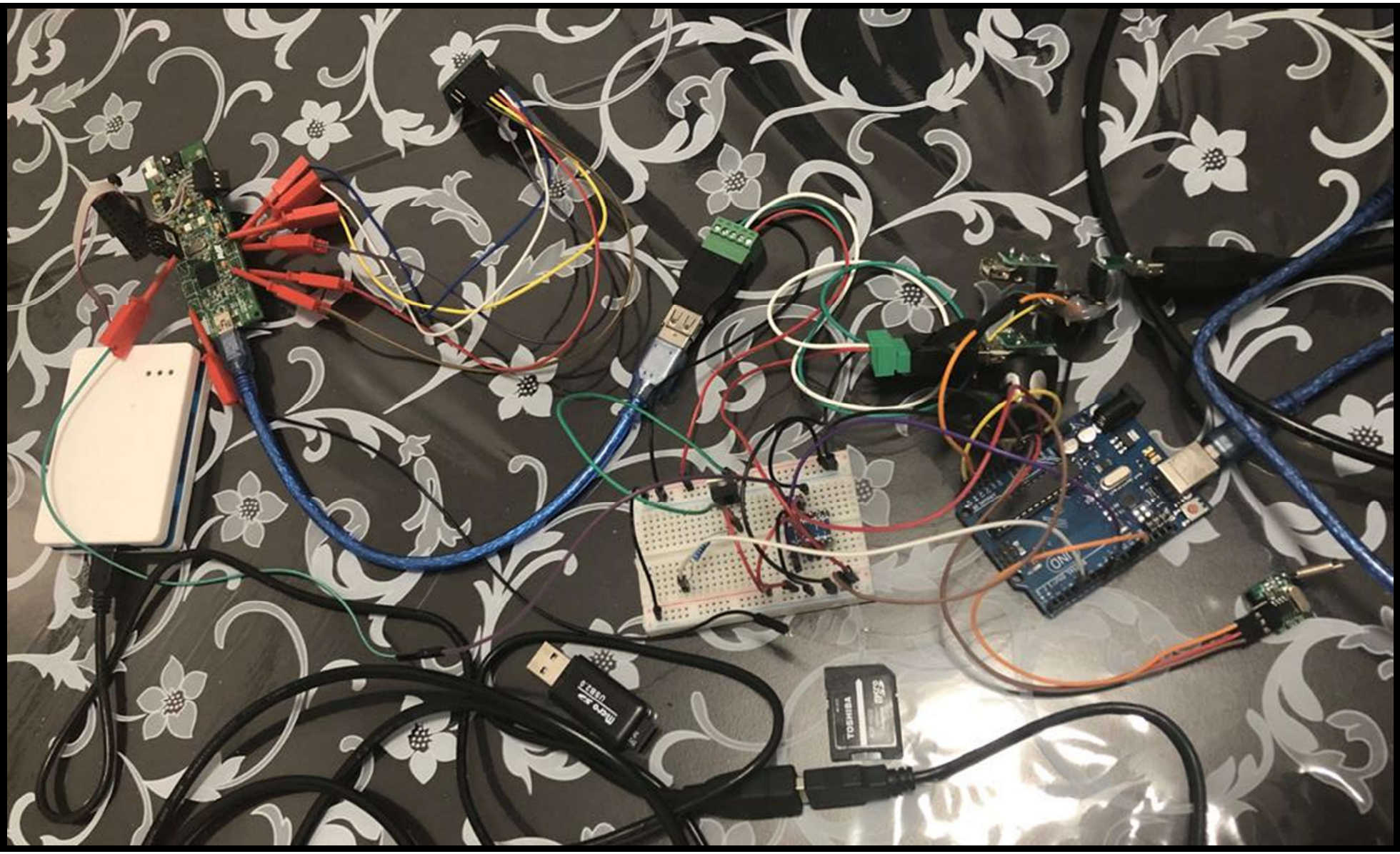
prototype shopping list 4

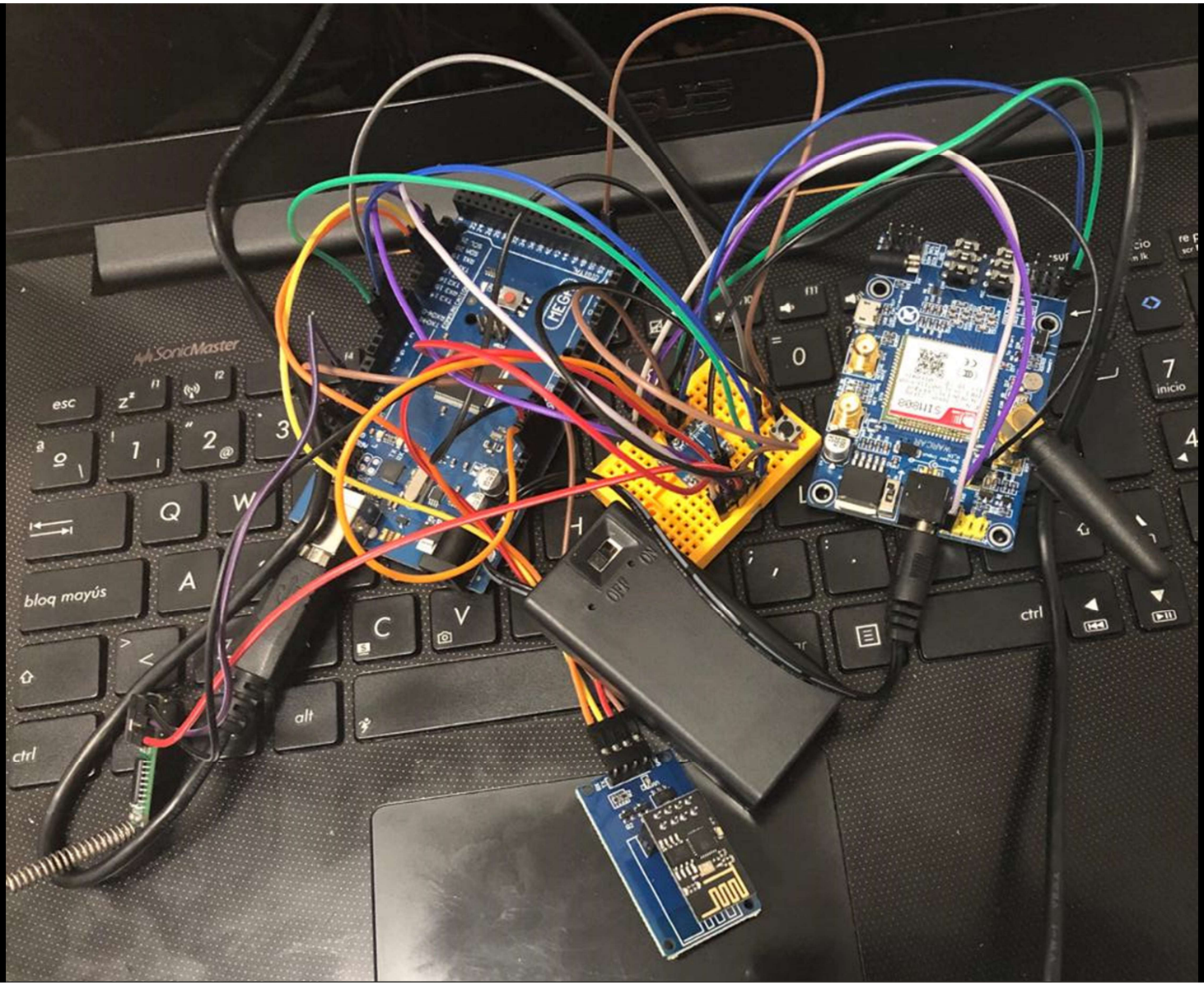
- Screw Kit Screw Driver
- Micro SD / TF Card Breakout to DIP Board Module (3.3v)
- Micro SD Module TF Micro SD Storage Board TF Card Memory Shield (5v)
- 120pcs 40PIN 20CM Dupont Line Male to Male, Female to Male, Female to Female Jumper Dupont Wire Cable
- AT90USBKEY2
- ATMEL ICE (ATATMEL-ICE)
- solder iron tip cleaning sponge pad
- Tin Lead Rosin Core Solder Wire

prototype shopping list 5

- Hot Air Glue Gun Thermo Electric Heat Temperature
- Test hook clip,Grabber SMD IC Test Probe Hook for Multimeter,Logic analyzer…
- 20pcs 10 pairs 40 Pin 1x40 Single Row Male and Female 2.54 Breakable Pin Header PCB




TOSHIBA

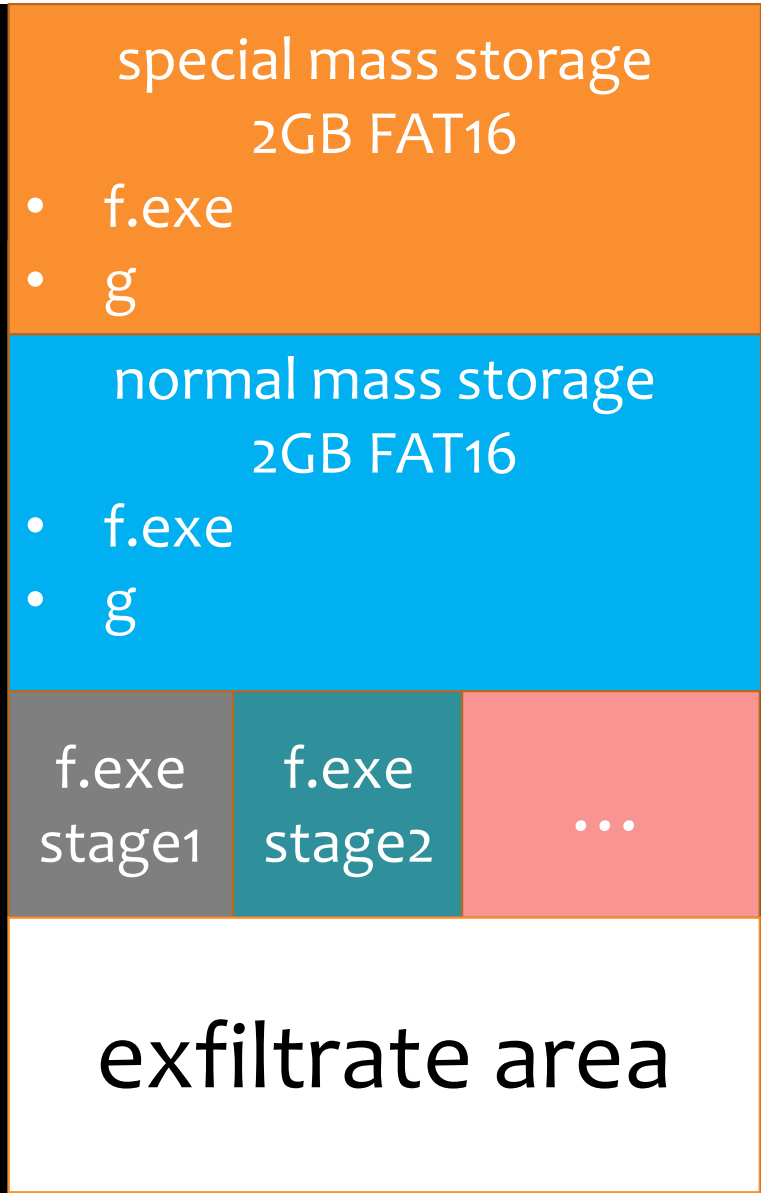

SonicMaster
esc
bloq mayús
ctrl
alt
ON
OFF

Roapt – my own pcb for attack

- soon available at www.rootkit.es
- JTAG, ICSP, UART…
- current beta prototype 1.0

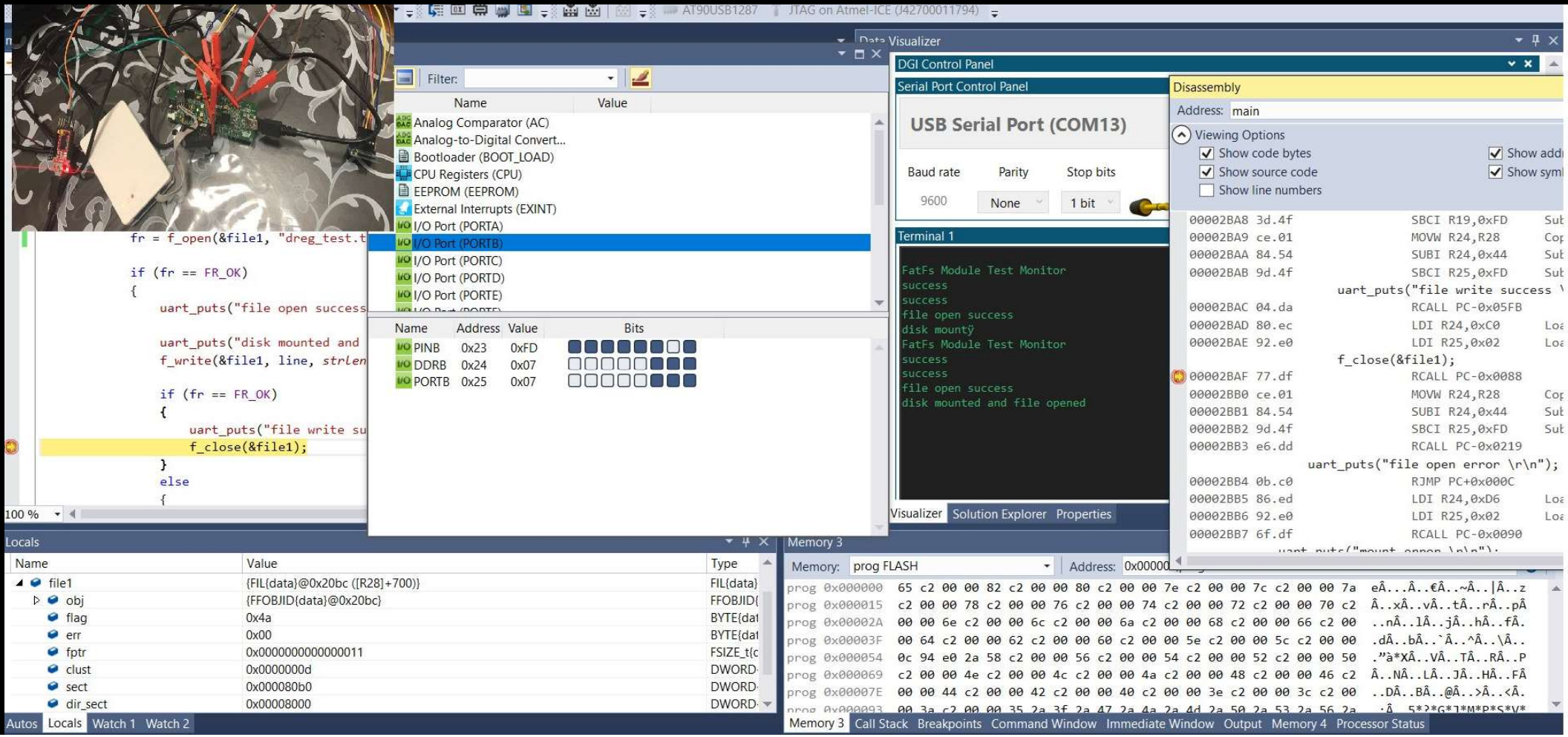
SD card SDHC 16GB

- FAT16, Only 1 FAT TABLE. **SPI is slow**
- f.exe: malware crypted – multi-stage
- exfiltrate blocks crypted from .exe
- g: file for communication with firmware. firmware can encrypt/decrypt sectors, relocate writes & reads, reset USB connection (OS cache), change stages, delete all f.exe entries..
- special area is “protected”
- Its possible switch between special-normal
- normal area can be formatted

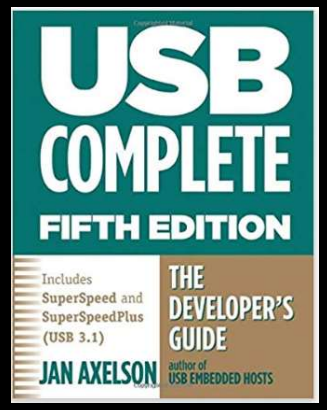


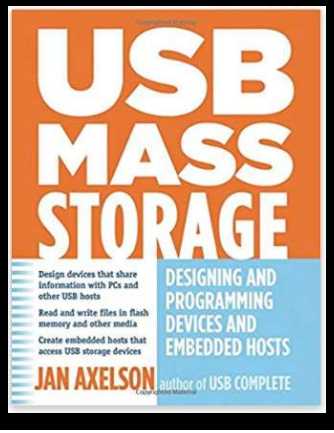
demo create & burn SD card image

demo firmware: dev, debug & flash. Atmel studio 7



- USB Mass Storage: Designing and Programming Devices and Embedded Hosts
- USB Complete: The Developer's Guide (Complete Guides series)
- https://www.microchip.com/DevelopmentTools/ProductDetails/PartNO/AT90USBKEY2
- https://www.microchip.com/wwwproducts/en/AT90USB1287
- https://www.avrfreaks.net/
- http://elm-chan.org/fsw/ff/00index_e.html
- http://www.fourwalledcubicle.com/LUFA.php





TO-DO

- improve source code: leaks, overflows, crap code…
- improve performance: fatfs, ISRs…
- more firmware & examples: SharpLocker/LockScream...
- more doc
- OS X & Linux examples
- more keyboard langs (current English)
- support multi-file (current POC is limited)
- exf mode selection: 433MHz(slow) or mass storage(faster)

Future (maybe)

- ARM Cortex-M4 180MHz 32 bit + rf transceiver
- NXP Kinetis *MK66**FN2**M0VMD18* or *MK66**FX1**M0VMD18*
- native 4bit-SDIO micro sd card port (SPI is very slow)
- cryptographic acceleration unit (AES) & CRC
- random number generator
- https://www.pjrc.com/store/teensy36.html
- NXP Kinetis FRDM-K66F board
- https://www.utasker.com/kinetis/FRDM-K66F.html

Greetz & credits

- janio IRC-HISPANO
- Sergio Lara & Luis Fernando Regel – Panda
- Jose Vicente Martínez – electronic engineering
- Paul Stoffregen - pjrc, teensy, altsoftserial…
- Mathieu Sonet: mass storage SD for Teensy2/ATMEGA32U4
- Dean Camera: lufa
- ChaN: fatfs
- Yassin Said Esteller

avrfreaks.net

Thx!

Questions?

evil mass storage in my github

- https://www.rootkit.es
- https://github.com/David-Reguera-Garcia-Dreg
- https://twitter.com/fr33project
- http://www.fr33project.org/
- dreg@fr33project.org