

Introducción al Hardware Hacking

DSR! - Indetectables.net
EkoParty 2022

Temario



1. Preparamos las Herramientas que vamos a usar
2. Analizamos el Hardware a atacar
3. Buscamos información útil
4. Planificamos el ataque

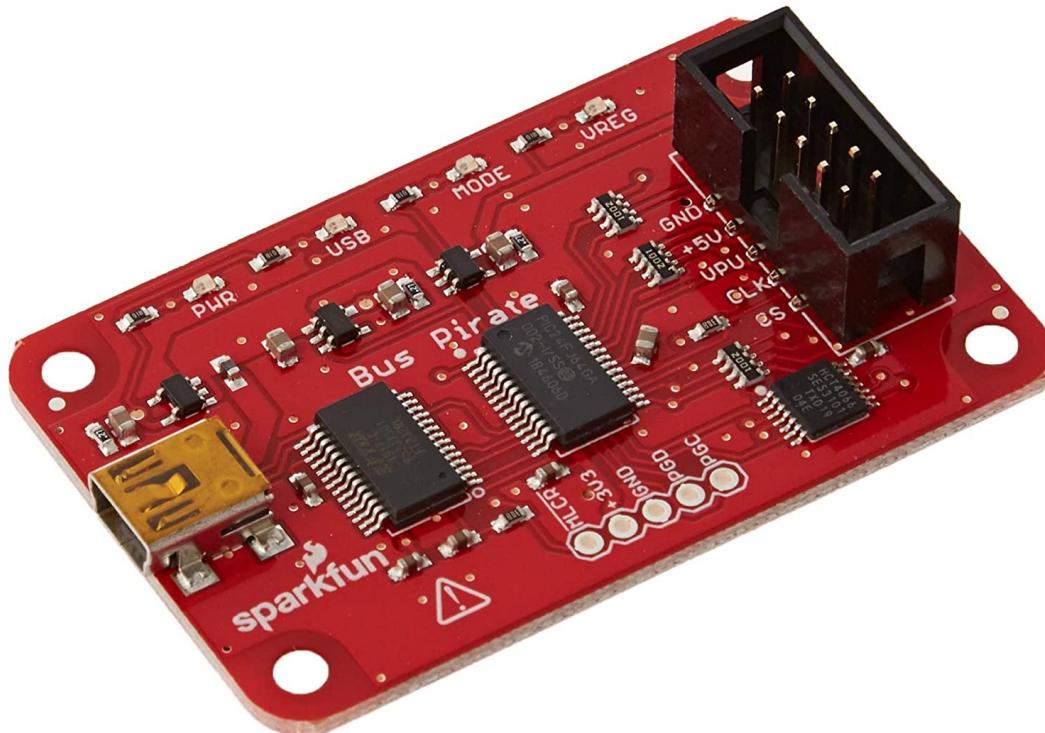
Referencias:

Foto de <https://github.com/yadox666/The-Hackers-Hardware-Toolkit>



Herramientas

Idealmente lo recomendable sería tener estas herramientas para poder superar cualquier obstáculo



1. De electrónica básica

- Multímetro
- Estación de soldado / soldador
- Destornilladores precisión
- Opening Tool, Opening Picks, Spudger, etc
- Flux, Kapton y papel aluminio

2. De microelectrónica

- Microscopio
- Pinzas Bruselas

3. De debugging

- PirateBus / Shikra / Generic UART Interface
- JTAGulator / JTAG debugger
- Flash Programmer



Analizando el Hardware

¿Qué buscamos?



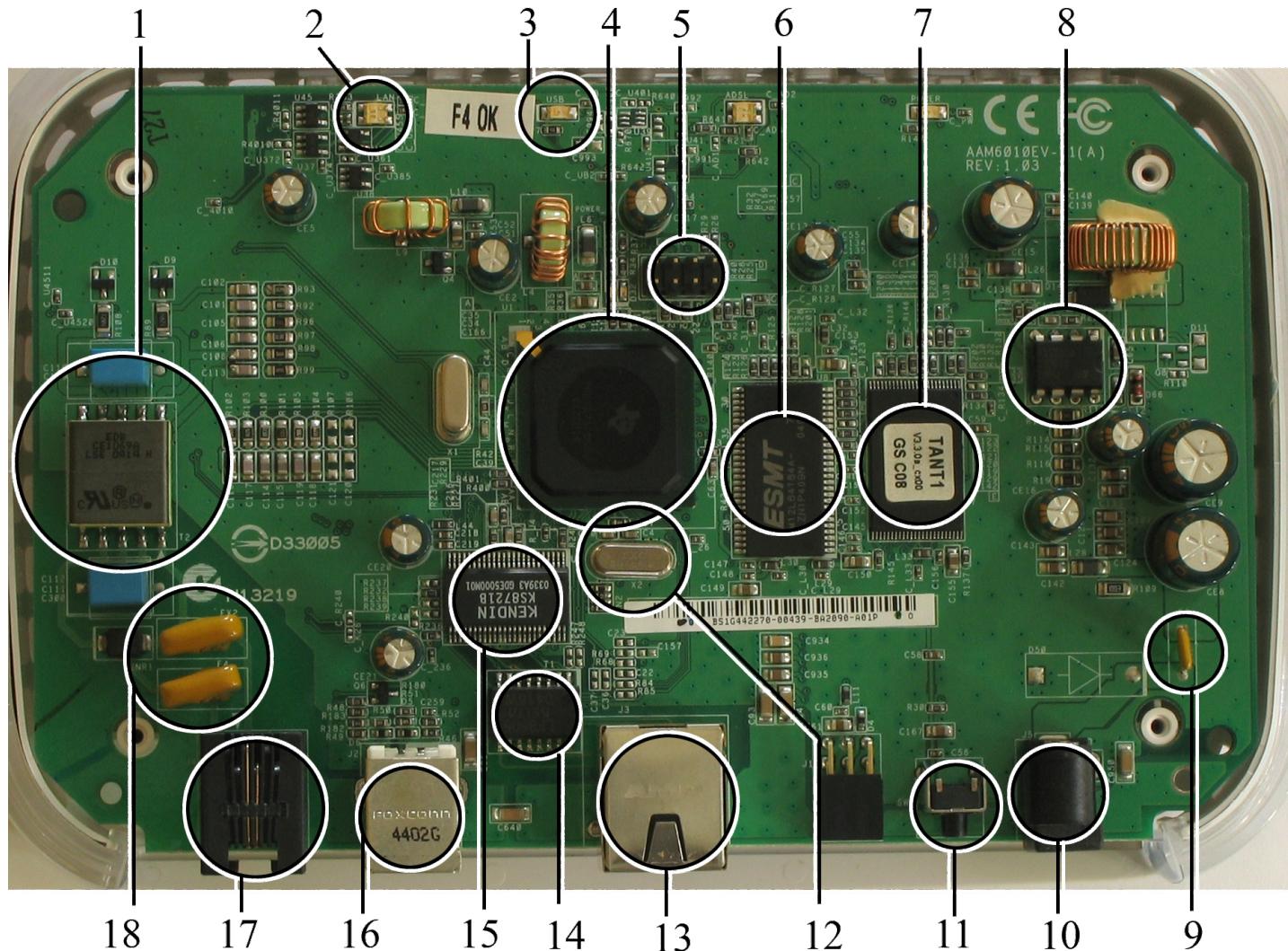
1. Ver como esta conformado el hardware
2. Buscamos puertos de debug
 - **UART**
 - **JTAG**: diseñado de tal manera que varios chips puedan tener sus líneas JTAG conectadas en daisy chain de manera tal que un solo "puerto JTAG" puede dar acceso a todos los chips del circuito impreso.



Analizando el Hardware

Netgear DG632 (ADSL modem/router)

- 1) Telephone decoupling electronics (for ADSL)
- 2) Multicolour LED (network status)
- 3) Single colour LED (USB status)
- 4) Main processor TNETD7300GDU
- 5) JTAG (Joint Test Action Group)
- 6) RAM ESMT M12L64164A 8 MB chip
- 7) Flash memory
- 8) Power supply regulator

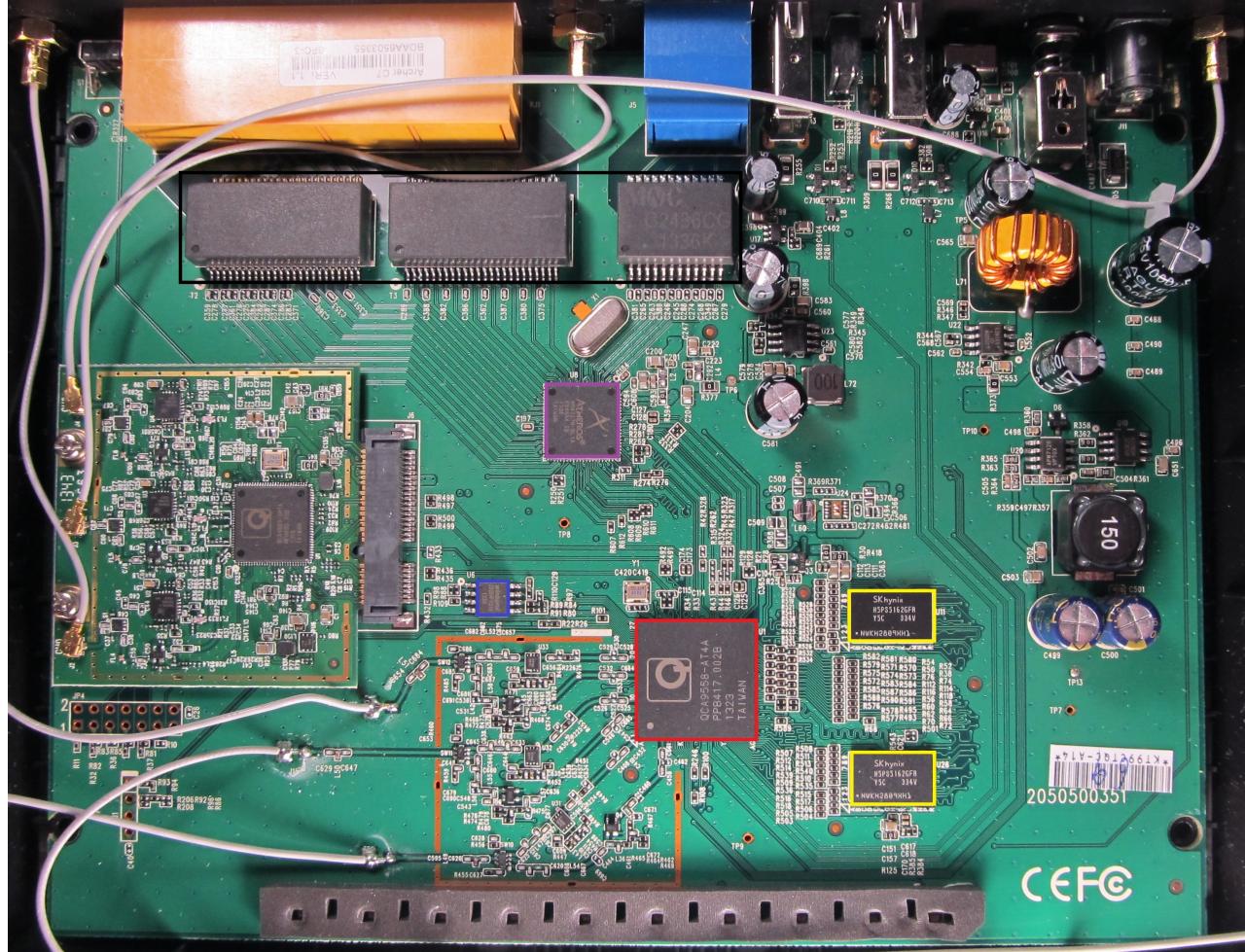


- 9) Main power supply fuse
- 10) Power connector
- 11) Reset button
- 12) Quartz crystal
- 13) Ethernet port
- 14) Ethernet transformer, Delta LF8505
- 15) KS8721B Ethernet PHY transceiver
- 16) USB port
- 17) Telephone (RJ11) port
- 18) Telephone connector fuses



Analizando el Hardware

TP-LINK Archer C7 v1



- WI SOC: QCA9558
- RAM: 128 MiB (SK hynix H5PS5162GFR-Y5C × 2)
- FLASH: 8 MiB (Winbond W25Q64FVSIG)
- SWITCH: Atheros AR8327N
- Network transformers

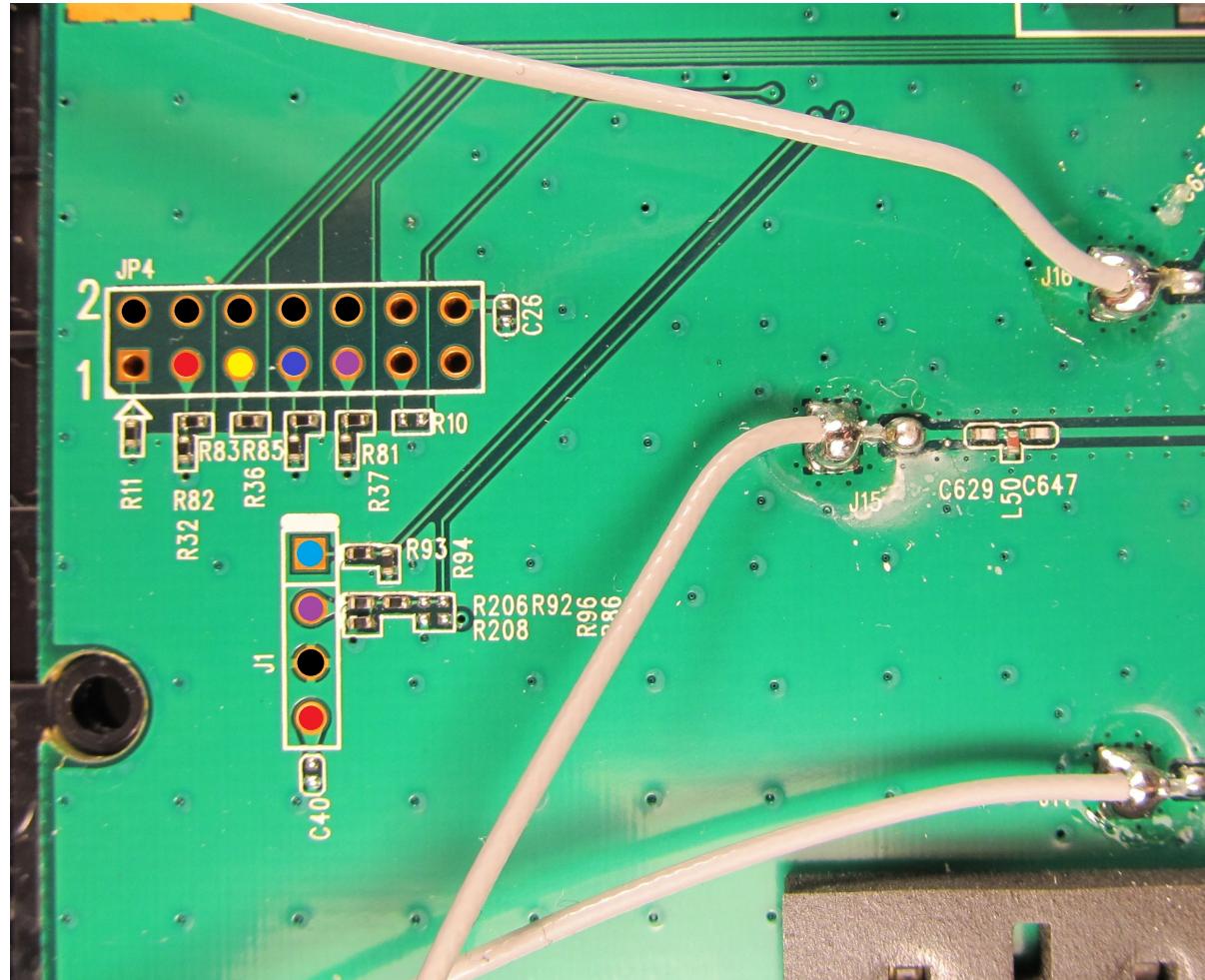
Referencias:

https://deviwiki.com/wiki/TP-LINK_Archer_C7_v1.x



Analizando el Hardware

TP-LINK Archer C7 v1



JTAG

- T_JTDI
- T_JTDO
- T_JTMS/T_SWdio
- T_JTCK/T_SWclk
- GND

UART/Serial

- RX
- TX
- GND
- VCC

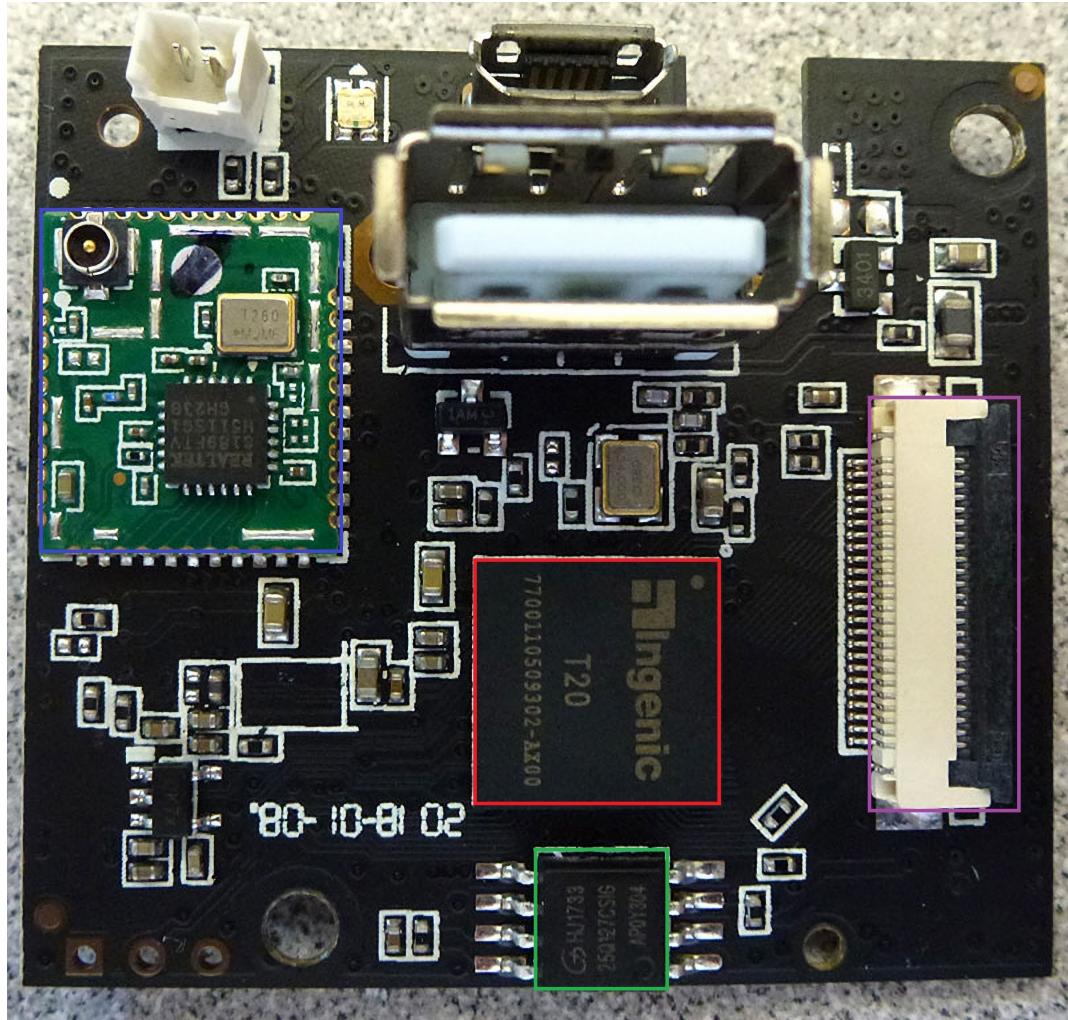
Referencias:

https://openwrt.org/toh/hwdata/tp-link/tp-link_archer_c7_ac1750_v1



Analizando el Hardware

Wyze Cam v2



- Ingenic T20 (Video Processor)
- FLASH: GD 25Q127CSIG
- WIFI module based on RTL8189ETV
- Camera module port

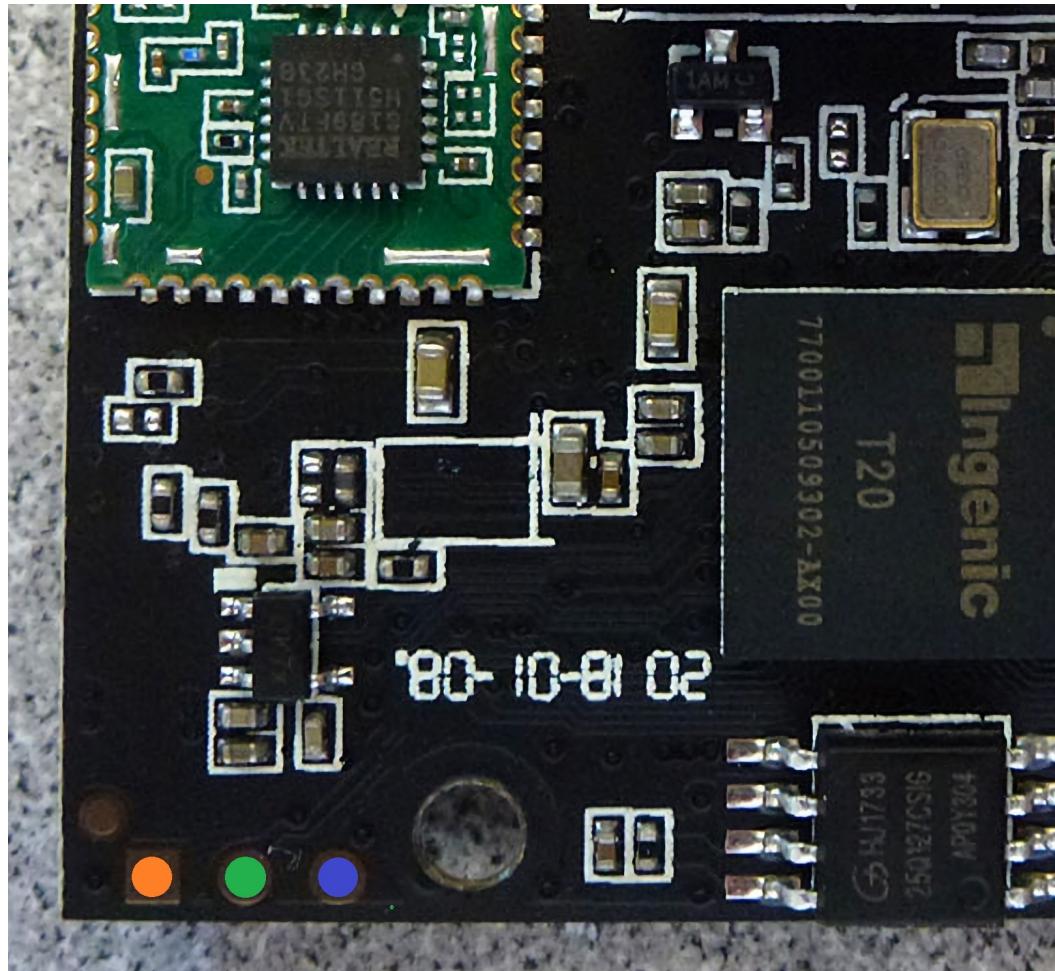
Referencias:

<https://www.edn.com/teardown-high-quality-and-inexpensive-security-camera/2/>



Analizando el Hardware

Wyze Cam v2



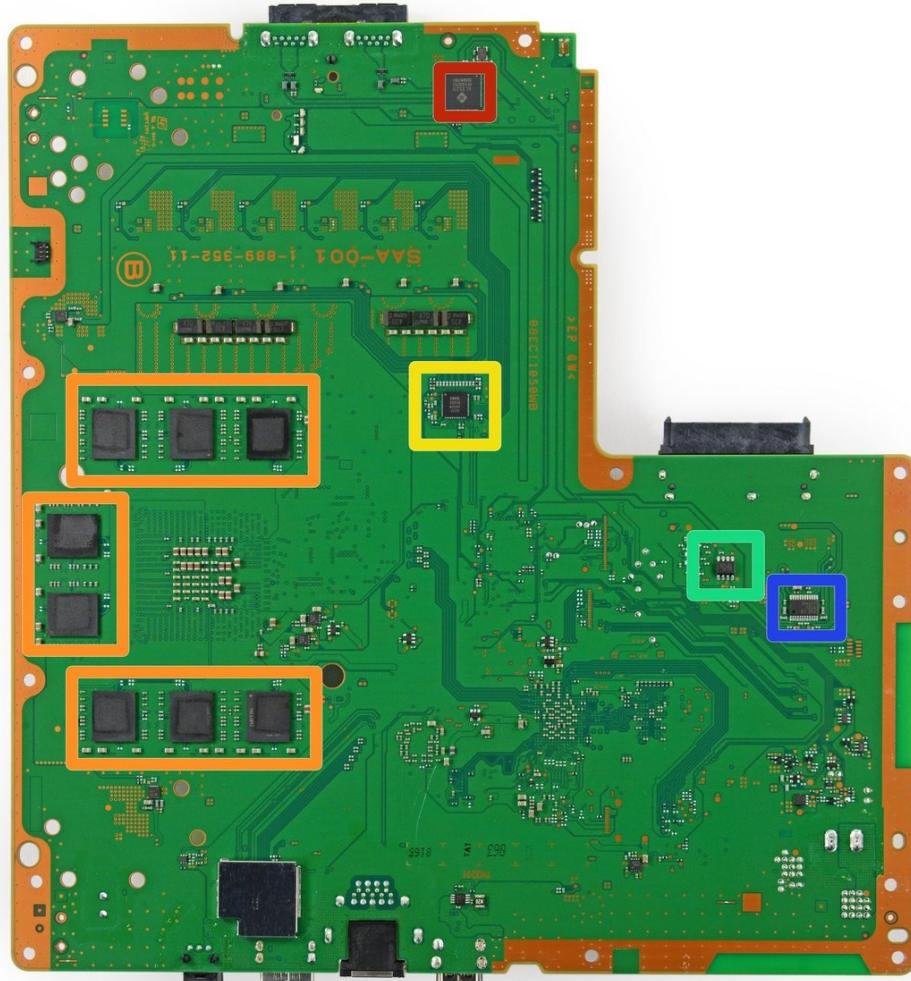
UART/Serial

- RX
- TX
- GND



Analizando el Hardware

PlayStation 4



- Genesys Logic GL3520 USB 3.0 Hub Controller
- International Rectifier 35858 N326P IC2X
- 39A207 1328 E1 3FU
- Samsung K4G41325FC-HC03 4 Gb (512 MB) GDDR5 RAM (x 8)
- Macronix 25L1006E CMOS Serial Flash Memory

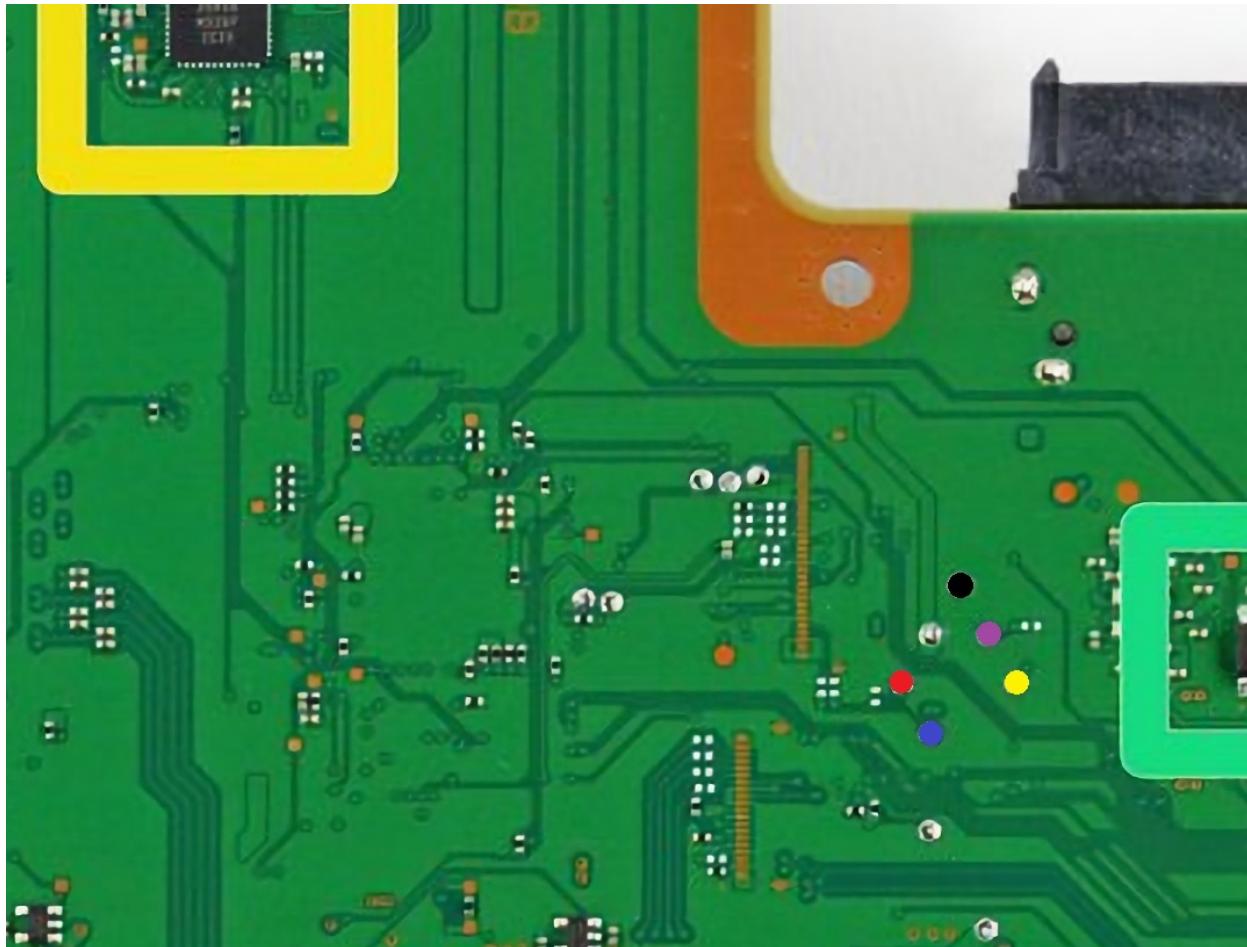
Referencias:

<https://www.ifixit.com/Teardown/PlayStation+4+Teardown/19493#s54790>



Analizando el Hardware

PlayStation 4



Aunque los puertos no estén marcados ni tengan fichas siempre pueden estar ahí escondidos en un test point

UART MEDIACON

- RX
- TX

UART 0

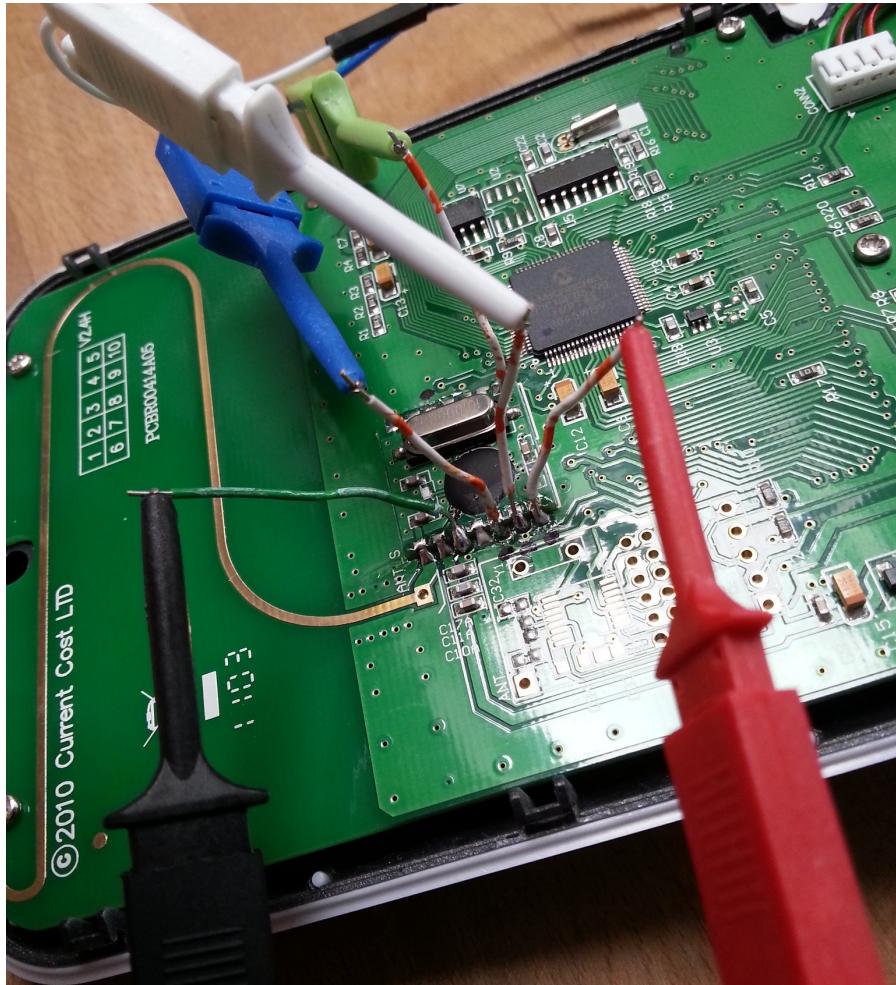
- RX
- TX
- GND

Referencias:

<https://hackinformer.com/2015/06/24/breaking-news-discovered-two-communication-ports-uart-playstation-4/>



Buscando información útil



1. Si tenemos logic analyzer
 - Sniffear las comunicaciones por spi
2. Si tenemos debug port
 - Vemos si hay información jugosa en los logs
 - Si el boot nos muestra el memory map buscamos particiones ocultas
 - Si la consola nos deja explorar el file system podemos espiarlo buscando credenciales, configuraciones, claves de cifrado, etc
3. Si tenemos cómo dumper la flash
 - Revisamos si podemos acceder a **particiones ocultas o configuraciones persistidas**
 - Revisamos los binarios buscando algún vector de ataque
4. Si tenemos como sniffear el tráfico
 - Intentamos obtener el fw que se instala cuando se updatea
 - Vemos que hace el hard con servidores o hard externo



Planificando ataques



Referencias:

Muchos de estos ataques se vieron en vivo en la DefCon 22

<https://www.youtube.com/watch?v=FJ7tutkij7A>



1. Si el target usa U-Boot
 - Si nos deja editar los bootargs intentamos podemos habilitar la consola
 - Si no está habilitado podemos intentar usar el “glitching attack” para usar la consola de emergencia
 - También podemos intentar dumper el fw con esto (Dumping Memory over Serial)
2. Si podemos actualizar el target
 - Si los updates no están firmados ni cifrados podemos hacer firmwares adulterados con ayuda de FirmwareModKit
3. Si el hard usa flash o eMMC
 - Si nos sirve para escalar las modificamos directamente
4. Si pudimos montar externamente el filesystem
 - Si hay dependencias que parecen explotables... les damos
 - Si el hard tiene un panel intentamos los típicos ataques de inyección de parámetros

¡Gracias por participar!

Si quieren ver más cosas de seguridad informática y desarrollo
están invitados a pasarse por la comunidad!

[Comunidad - Discord](#)

