

/Rooted®



HARDWARE HACKING + SOLDERING SKILLS + FIRMWARE REVERSING WITH GHIDRA + SDR RADIO

MADRID

4 al 6 de Marzo de 2024

DOSIER DE FORMACIÓN

A group of people are gathered around a table in a dimly lit room, likely a hackathon or a computer lab. They are focused on their laptops and mobile devices. The scene is illuminated by the glow of the screens and some ambient light. The text "/Rooted" is overlaid in the center in a large, white, sans-serif font. The slash is a simple forward slash, and the 'o' in "Rooted" has a registered trademark symbol (®) next to it. The background is dark, with some blurred lights and the silhouettes of other people.

/Rooted®

/Rooted[®]

Días 4-6 de Marzo

Tres días de trainings y workshops

*HOTEL Eurostars iHotel
Pozuelo de Alarcón*

Días 7-9 de Marzo

Ponencias presentadas por speakers internacionales y expertos técnicos.

*KINEPOLIS
Pozuelo de Alarcón*

Presentación

- **Misión:** queremos compartir conocimientos, atraer diferentes culturas, exponer el talento local y marcar la diferencia.
- **Visión:** ser responsables haciendo algo diferente, compartiendo cultura y construyendo una red de conocimiento. Ser un evento honesto, confiable, beneficioso y establecer alianzas y colaboraciones con socios, clientes y competidores.
- **Nuestra cultura ganadora y nuestros valores en vivo:** colaboración, diversidad, talento por todas partes, pasión, calidad y enfoque en los clientes (cada persona que asiste a nuestros congresos).

David Melendez Cano

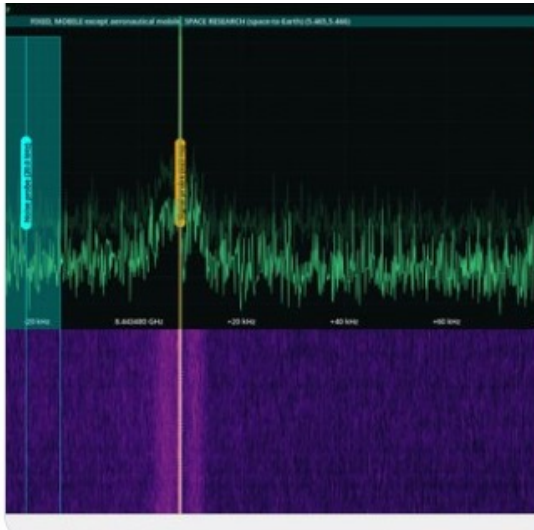
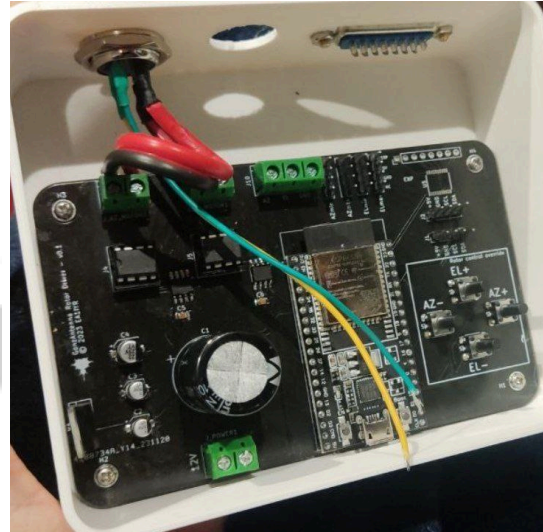
/Rooted[®]

R&D Embedded Software | DEFCON
USA Speaker, BlackHat | Maker | Book
author: "Hacking con Drones"

Project "*The Interceptor*"



ot



Gonzalo J. Carracedo

Profesional de la informática con 7 años de experiencia y actualmente cursa el doctorado en Astrofísica por la Universidad Complutense de Madrid.

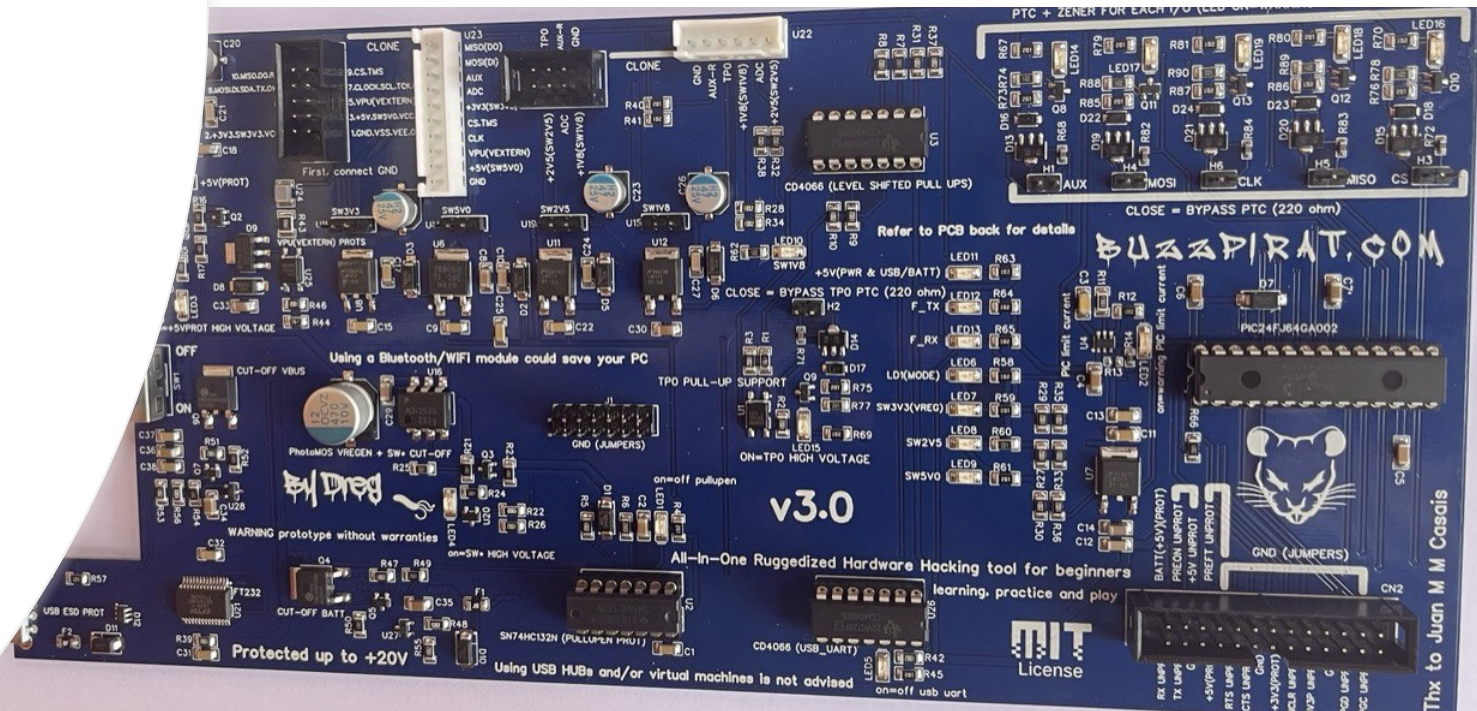
Anteriormente fue consultor de ciberseguridad (y más tarde, responsable de Innovación) en la firma española Tarlogic Security. Su experiencia abarca desde el desarrollo de software hasta la ingeniería inversa y hardware hacking (con especial interés en las comunicaciones por radiofrecuencia).

Ha impartido charlas y talleres en congresos de ciberseguridad como RootedCON, EkoParty o GSICKMinds. Ocupa su tiempo libre desarrollando SigDigger, una herramienta gráfica de análisis de señales digitales que intenta acercar tanto a aficionados como a profesionales al mundo del SDR.

David Reguera Garcia

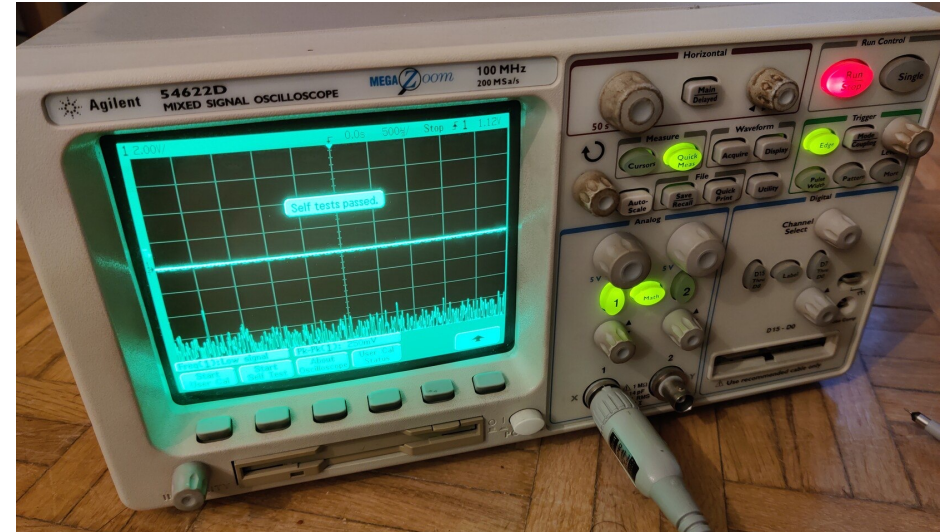
Senior Malware Researcher, OS Internals, C/C++, x86 x64 ASM, reversing, forensics, hardware hacking, AVR, PIC, ARM Cortex, Founder & CEO at rootkit.es

ootae



Antonio Vazquez Blanco

Profesional especializado en investigación de ciberseguridad con un enfoque apasionado en electrónica y ingeniería inversa. Poseo una amplia experiencia en sistemas de bajo nivel y tecnologías bare metal, lo que me permite abordar desafíos complejos en el campo de la seguridad informática. Actualmente, estoy expandiendo mis conocimientos en el ámbito de la radio amateur y el procesamiento avanzado de señales, buscando innovar y aplicar estas habilidades en proyectos de ciberseguridad



Roote

Cristina Casas Sastre

ootae



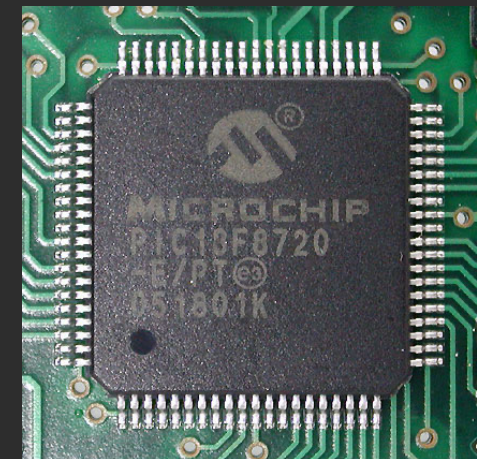
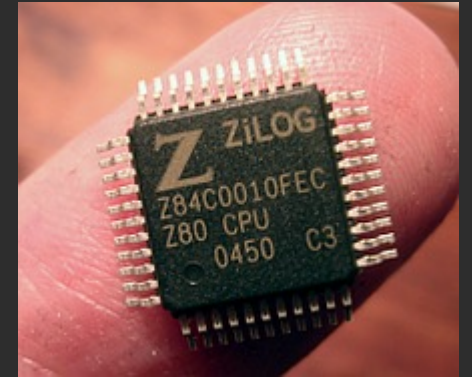
De formación soy química, pero rápidamente me empecé a dedicar profesionalmente a la informática y en concreto a las disciplinas dedicadas al dato, evolucionando desde el Business Intelligence hasta la Ciencia de Datos más experimental. Hoy en día soy analista y desarrolladora en StratioBD, especializada en Gobierno del Dato orientado a IA Generativa. Durante el último año me he introducido en el mundo del Hardware Hacking, y de todas sus vertientes me he quedado con la soldadura SMD. Mi siguiente gran objetivo es empezar a diseñar mis placas y así seguir cultivando esta nueva pasión.

Objetivos

- Curso para gente sin conocimiento de: IOT, de/soldar, hardware hacking, radio, reversing, electrónica y matemáticas
- ¿Tienes un cacharro IOT y quieres extraer + entender su firmware? ¿Auditar IOT?
- ¿Quieres intentar modificar/reparar/reemplazar el chip BIOS de PC?
- ¿Quieres obtener habilidades: radio, soldar+desoldar & hardware hacking? TE DAMOS TODAS LAS HERRAMIENTAS
- ¿Quieres intentar hacer un MOD a tu router/consola/impresora 3D/patinete....?
- ¿Aprender lo básico de electrónica para no prender fuego a la casa todo el rato?
- ¿Cómo usar bus pirate v3 y otras herramientas famosas para hardware hacking / IOT?
- ¿Qué es JTAG, UART, I2C, SPI...? ¿I2C EEPROM vs SPI FLASH? ¿3,3v? ¿5v? ...
- ¿Satélites? SDR + microondas + sondas de la NASA
- ¿Reversing de firmware + ASM básico con GHIDRA?

Algunos de los Objetivos

- Buscar JTAG, UART...
- Aprender a usar Bus Pirate v3 de manera profesional: I2C EEPROM, SPI FLASH..
- Uso de analizador lógico
- Asprogrammer, flashrom, binwalk
- soldar+desoldar con JBC14st: pines macho+hembra, QFP, SOT23, SO14, resistencias, condensadores..
- soldar+desoldar con pasta y pistola: tips & tricks
- Cambiar pines macho por pines hembra en una fila entera...
- Uso del multímetro básico
- RADIO SDR
- Reversing firmware con GHIDRA + ASM



A quién va dirigido

- ¿¿¿Tienes curiosidad sobre radio, firmware reversing, hardware hacking + cómo soldar/desoldar???
- ¿¿¿No sabes por dónde empezar, ni que material comprar???
- Te damos todo lo necesario
- Este bootcamp es **APTO** para gente que no tiene ni idea de:
 - Hardware
 - Electrónica
 - Matemáticas
 - Soldar/Desoldar
 - RADIO SDR
 - Reversing
 - ASM
- Es complementario al bootcamp de la edición 2022 & 2023: se darán materiales/herramientas/hardware nuevo/diferente y además el temario tiene algunas cosas nuevas ;-)

Requisitos: Conocimientos

Conocimientos básicos de:

- ✓ Uso de Linux+Windows nivel usuario (consola)
- ✓ Informática básica: bits, bytes
- ✓ Saber leer en inglés
- ✓ Curiosidad
- ✓ Ganas de aprender y de practicar con las manos
- ✓ ¿Algo de Python?

Requisitos: Técnicos

Para el correcto funcionamiento del training será necesario que los alumnos dispongan de equipos con acceso de administrador para poder añadir, eliminar software o cambiar cualquier configuración del mismo.

Las máquinas deben contar con las siguientes características mínimas:

- ✓ Linux+Windows (**DUAL BOOT**) instalados de manera **NATIVA** (preferible Ubuntu + Windows 11).

*Si no sabes hacerlo trae el ordenador formateado y te ayudamos el **PRIMER DÍA**

Agenda (i)

El primer día: aprender a soldar, desoldar, usar la pistola, “cosas manuales”, IOT...

El segundo día: haremos hardware hacking con bus pirate v3, ch341, analizador lógico, buscar jtags, UART... y todo lo que nos dé tiempo 😊

El tercer día: firmware reversing con GHIDRA, satélites, ¿Satélites? RADIO SDR + microondas + sondas de la NASA...

Iremos aprendiendo cosas de electrónica, radio.... sobre la marcha, usando un lenguaje sencillo y sin matemáticas ni cosas complicadas

Agenda (ii)

IMPORTANTE: Para nosotros es VITAL que todos los asistentes aprendan y puedan seguir el ritmo curso. Si es necesario dejar algo de temario fuera del curso **lo haremos**

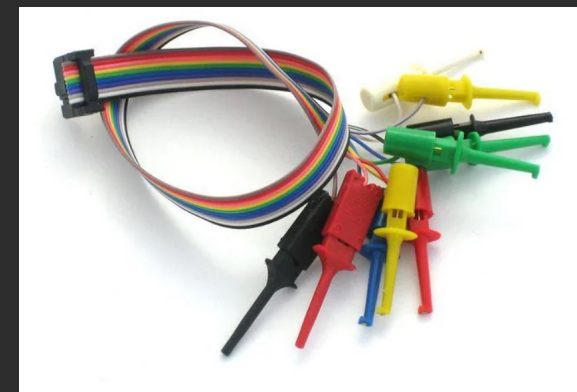
PACIENCIA! Hay personas más torpes con las manos, con más dudas, otros tendrán problemas usando las aplicaciones, problemas con drivers etc. Nuestro objetivo es que lo más importante quede claro y aprendido para **TODOS** los asistentes

Para que podáis seguir aprendiendo por vuestra cuenta os daremos: material complementario, documentación, enlaces...

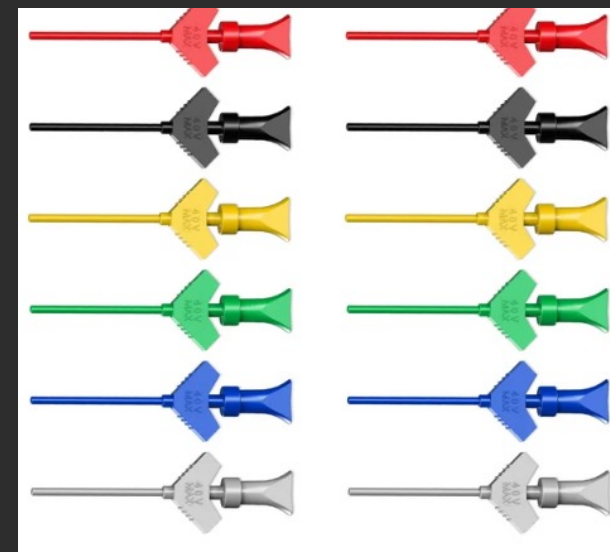
* es posible que algunas cosas sean reemplazadas por otras según disponibilidad / problemas varios

/Rooted®

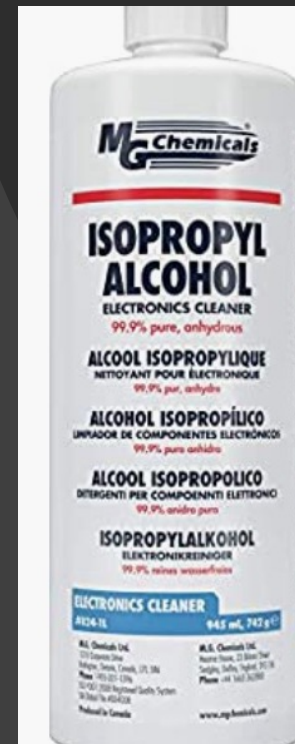
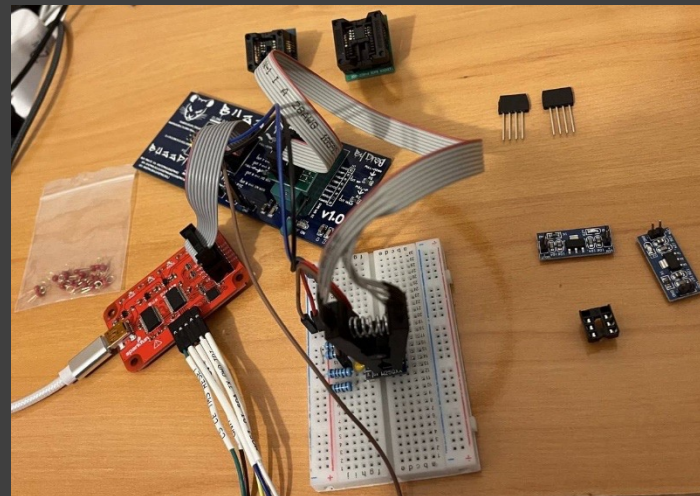
Fotos de lo que te llevas a casa I



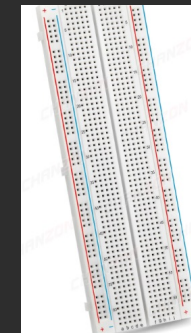
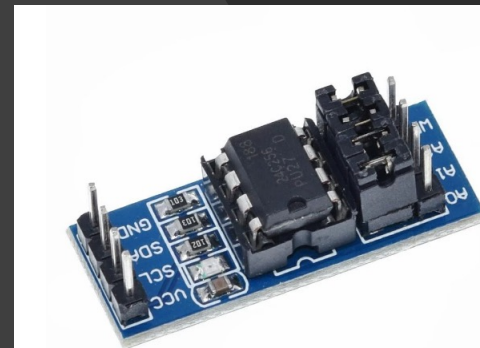
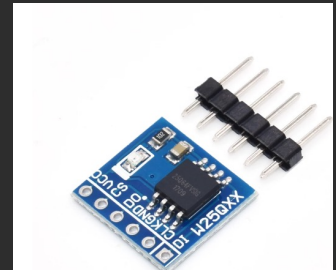
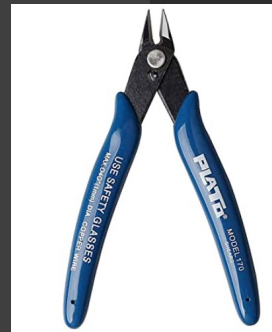
En el precio viene incluido ~1000 EUROS en material (herramientas de CALIDAD)



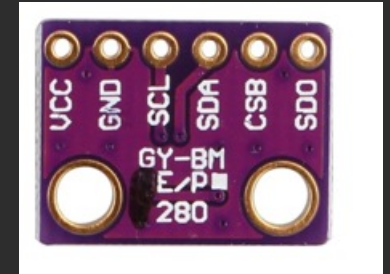
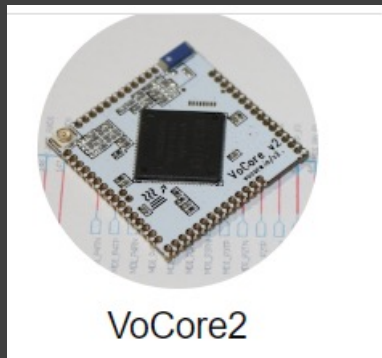
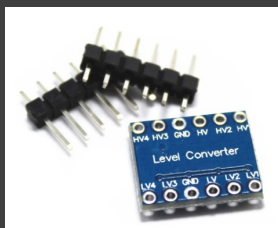
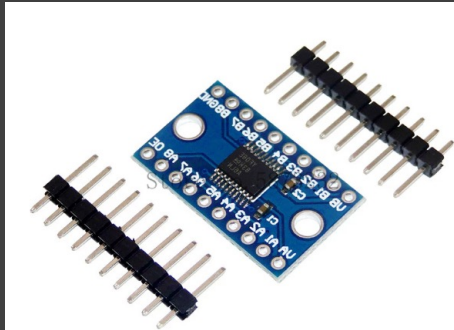
Material que te llevas a casa II



Material que te llevas a casa III

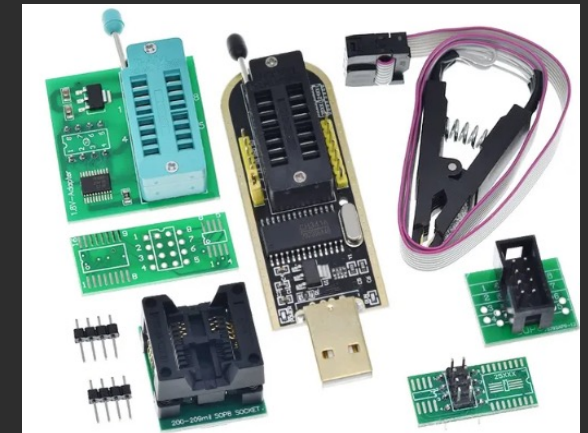
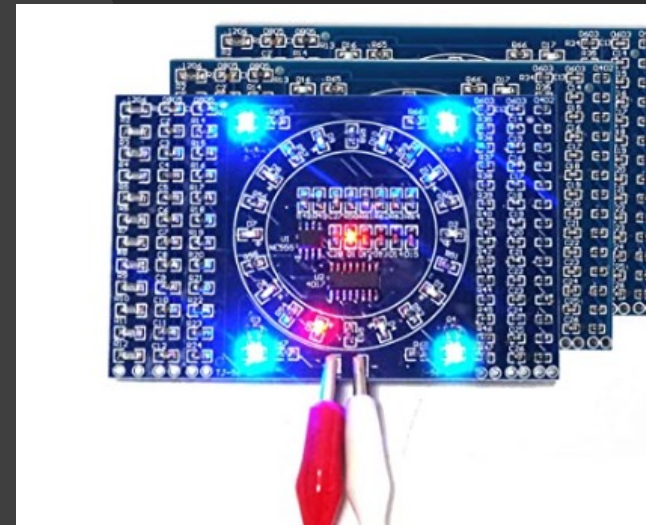


Material que te llevas a casa IV



Material que te llevas a casa V

- + Alguna cosita/sorpresa más ;-)



* Debido a la crisis mundial de chips/componentes/materiales... es posible que algunas cosas sean reemplazadas por otras según disponibilidad

Lista de algunos de los materiales

UN Alcohol Isopropolico MG Chemicals IPA, UNA Botella pulverizadora, UN Pack pines hembra + pines macho HEADER, UN Bus pirate v3, UN Bus Pirate 3 Cable Kit, Un buzzif kit, UN Analizador lógico USB 24MHz 8 canales, UNA SPI FLASH W25Q64 3.3v, UNA EEPROM I2C AT24C256 5v, UN AZDelivery ATmega328P 5v, UN Kit cables DUPONT (macho hembra, macho macho, hembra hembra), UN JBC 14ST, UN ESTAÑO TRIMETAL MBO 0.5mm 100gr, UNA PASTA DE SOLDAR, UN FLUX JBC FL-15, UN KIT Clip de prueba SMD IC 12 PCS, UNA Estación de Trabajo 858D, UN MG Chemicals 424-NS Super Wick No Clean, UN Microscopio Digital AD407 7 pulgadas, UN Tapete de silicona para soldar, UN Desoldador manual, UN Cable USB C – USB A 15 cms, UN Paquete de 8 pilas AA Duracell, UN Paquete de 8 pilas AAA Duracell, UNA Tercera mano con lupa + soporte soldador, UN Alicates de Corte Diagonal, UN TXS0108E conversor voltaje bidireccional de 8 canales 3,3v <-> 5v, UN conversor voltaje bidireccional de 4 canales 3,3v <-> 5v, UN CII I2C, UN SOLDADOR ELECTRICICO DE 60W EU-PLUG, UN KIT MÁS DE APRENDE A SÓLDAR SMD/SMT, UN KIT PRINZAS DE PRECISIÓN, UNA Protoboard, UN MULTÍMETRO DIGITAL, UN VoCore2, UN BMP280 Barometric Pressure Sensor Module, un kit RTL-SDR....

Costes

- El precio final de este Bootcamp + entrada al Congreso RootedCON es **1750 €**
- Si quieres asistir al curso sin que te compremos el material (no estas interesado en la parte manual): Bootcamp sin el material + entrada al Congreso RootedCON es **980 €**
- Puedes registrarte y formalizar el pago en: <https://reg.rootedcon.com>

IMPORTANTE:

Se requiere un mínimo de **SEIS (6)** asistentes para que el curso pueda celebrarse.

MÁXIMO 20 alumnos. Queremos poder dar atención personalizada a cada asistente.

FAQ

- **Dónde se celebra la formación?**
 - A diferencia del Congreso RootedCON, las formaciones se celebran en el Hotel Eurostarts i-Hotel
 - Aquí puedes encontrar el mapa de la zona: [Google Maps](#)
- **Qué diferencia hay entre BootCamp y RootedLab?**
 - Diferenciamos los training por horas de formación. Un RootedLab tiene 8 horas de formación, mientras que un BootCamp tiene unas 24h.
- **Qué horario tiene la formación?**
 - La formación comienza a las 9 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8 :)
 - Las formaciones suelen acabar entre las 19h y 20h.
- **Como puedo registrarme?**
 - Para el registro, ve directamente al [RootedManager](https://reg.rootedcon.com): <https://reg.rootedcon.com>. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados.
- **Puedo pagar con transferencia bancaria?**
 - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- **El training incluye comida?**
 - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted®

