



La Guía del Wardriving con Open Hardware

-
- Adrian González (d3vnulv01d)
 - Berenice Ávila (backdoorbabyyy)

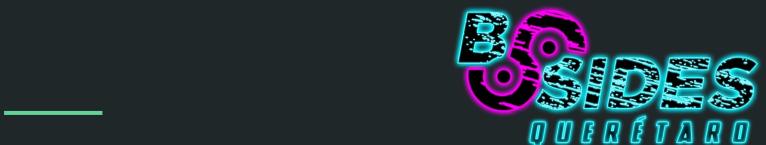
\$ about us

- Ingenieros en Sistemas Computacionales (IPN ESCOM & Club de Seguridad Informática)
- Red Teamer/AppSec & Desarrollador de Software
- Aprendices apasionados de romper cosas y aplicaciones.
- Aprendices en todo, expertos en lo que caiga.



\$ Contenido

- Hardware para seguridad
- ¿Qué es el wardriving?
- ¿Qué es el open hardware?
- Hardware para wardriving
- Opciones no open hardware
- Demos



\$ Disclaimer

La información y demo es meramente con fines educativos para la creación de espacios de aprendizaje de redes inalámbricas y de dispositivos que usan alguna radio frecuencia, toda información de la demo mostrada será eliminada. También de su mentes.



\$ ¿Qué es el wardriving?

El "wardriving" es el acto de buscar redes y dispositivos que emitan alguna radio frecuencia de manera pasiva. (BLE, IoT, Telefonía, RF). Sin intervención o con interrupción de las señales emitidas



Wardriving

What my friends think I do

What my mom thinks I do

What society thinks I do

What my boss thinks I do

What I think I do

What I actually do

\$ ¿Qué es el Open Hardware?



- Son diseños de dispositivos electrónicos que cuentan con una licencia la cual permite ser replicados y estudiados
- También son aquellas placas o proyectos que usan componentes que puedan tener una licencia privada, pero que en su diseño final se puede estudiar y replicar



\$ Hardware para wardriving



\$ Opciones libres

System on Chip (Soc)

- Raspberry Pi (Software/Firmware)
- Nvidia Jetson (Software)
- Orange Pi (Software/Firmware)
- ESP 32 (Firmware)
- Arduino Q (Firmware/Software)

Hats

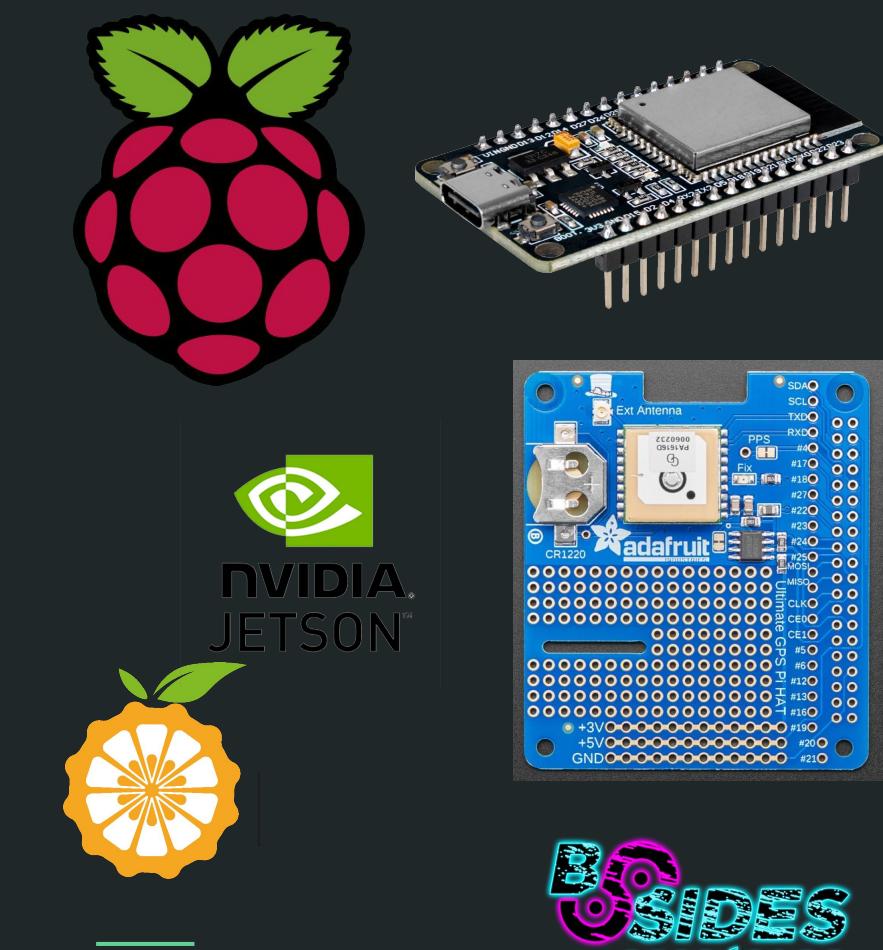
- GPS
- Adaptadores de otros protocolos

Almacenamiento

- Micro SD
- M.2
- Por comunicación hacia otro dispositivo (BLE, WiFi, IoT)

Herramientas

- Minino
- Flipper Zero + Módulo WiFi + GPS
- DIY (Firmware/Software)



BO
SIDES
QUERÉTARO

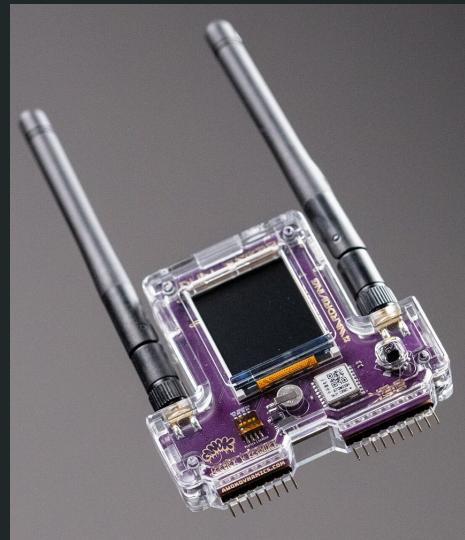
\$ Opciones no Open Hardware

System on Chip (Soc)

- ESP 32 en versiones de herramientas all in one con otras antenas o placas de desarrollo sin acceso a sus esquemáticos
 - Marauder ESP 32
 - BFFF
 - AWOK ESP 32

Cualquier otra herramienta o antena que no cuente con diagramas o su firmware abierto para estudio.

Nota: A menos que hagas reversing o hardware hacking comparte y haz crecer la comunidad.



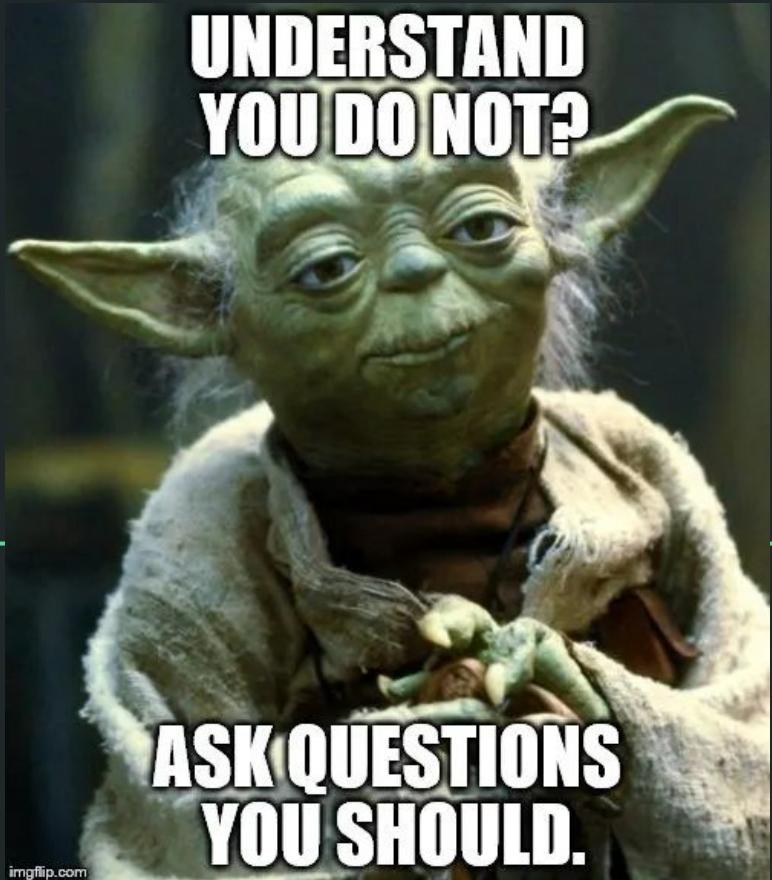
\$ Demos



\$ Spoiler:

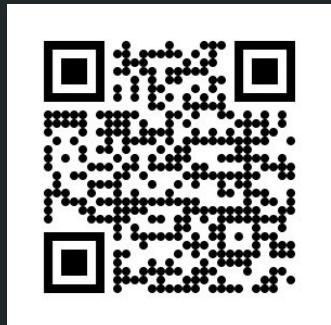


\$ Dudas, preguntas



\$ Muchas gracias por su atención.

Contactos:



Proyecto:

