HARDWARE · MAPEO DE REDES WIFI CON ESP32

ESP32 + GPS: mapea redes inseguras por $9

Cómo un chip de $9 dólares puede detectar redes WiFi abiertas, configuraciones débiles y puntos de acceso falsos en toda tu ciudad — de forma completamente pasiva y legal.

01 — ¿QUÉ ES EL WARDRIVING CON ESP32?

Mapeo pasivo de señales WiFi en movimiento

Wardriving es la práctica de moverse por un área mientras se capturan señales WiFi con un dispositivo receptor. Con un ESP32 y un módulo GPS puedes registrar todas las redes visibles con sus coordenadas exactas, generando un mapa de la seguridad WiFi de tu ciudad. Es 100% pasivo — solo escucha, nunca emite señales atacantes.

Técnica documentada desde 2001 · Legal en modo pasivo en México · Compatible con WiGLE.net

$9	360°	100%
USD hardware ESP32 — disponible en MercadoLibre México	cobertura de señal WiFi en movimiento continuo	pasivo — nunca emite señales ni desautentica usuarios

02 — HARDWARE NECESARIO (MENOS DE $30 USD TOTAL)

ESP32 (principal)

$9 USD

Microcontrolador con WiFi 802.11 b/g/n integrado. Dual core 240 MHz, BLE, 4MB flash. Captura beacons de todas las redes visibles en tiempo real.

`MercadoLibre · Arduino IDE · SDK oficial`

Módulo GPS (Neo-6M)

$8 USD

Proporciona coordenadas de latitud y longitud exactas en tiempo real. El ESP32 combina cada red detectada con su posición GPS para el mapa final.

`Neo-6M · Neo-8M · UART · 9600 bps`

Módulo MicroSD

$5 USD

Almacena los datos en formato CSV compatible con WiGLE y herramientas de mapeo. Capacidad de miles de redes por sesión de wardriving.

`SPI · FAT32 · CSV export`

Power bank estándar

Ya tienes uno

El ESP32 consume ~180mA. Un power bank de 5,000 mAh da más de 15 horas de operación continua — suficiente para mapear toda una ciudad mediana.

`5V USB · ~180mA consumo · 15+ horas`

03 — QUÉ PUEDE DETECTAR Y POR QUÉ IMPORTA

Redes WiFi abiertas sin cifrado

Detecta todos los SSIDs que no usan cifrado. En estas redes, cualquier persona conectada puede ver el tráfico de los demás usuarios — contraseñas, correos, datos bancarios si no usan HTTPS.

`Sin contraseña → Sin cifrado → Datos expuestos`

Redes con WEP (protocolo obsoleto desde 2004)

WEP puede crackearse en menos de 60 segundos con herramientas básicas. Si un negocio o casa sigue usando WEP, su red está prácticamente abierta. El ESP32 identifica el tipo de cifrado de cada red detectada.

`WEP crackeable en <60 segundos`

Redes Evil Twin — SSIDs duplicados sospechosos

Detecta cuando el mismo nombre de red (SSID) aparece con diferentes MACs en el mismo área — señal clásica de un ataque Evil Twin donde alguien creó una red falsa con el mismo nombre que la legítima.

`⚠ Indicador de ataque activo en el área`

Redes corporativas con configuración débil

Identifica redes empresariales usando WPA/WPA2-Personal en lugar de WPA2/WPA3-Enterprise. Las redes corporativas deberían usar autenticación por certificado, no contraseña compartida.

`WPA2-Personal vs WPA2-Enterprise`

Mapa visual de densidad y seguridad WiFi

El CSV generado es compatible con WiGLE.net y Google Maps. Puedes visualizar un heat map de densidad de redes en tu ciudad, filtrando por tipo de seguridad para identificar zonas de riesgo.

`WiGLE · CSV · KML · Google Maps`

04 — CÓMO CONSTRUIRLO PASO A PASO

01 — Conecta ESP32 + GPS + MicroSD

El GPS se conecta vía UART (TX/RX). El módulo SD vía SPI (MOSI, MISO, CLK, CS). Alimenta todo desde el pin 3.3V o 5V del ESP32. Sin soldadura necesaria si usas módulos con pines.

`GPS: TX→GPIO16, RX→GPIO17 · SD: CS→GPIO5`

02 — Flashea el firmware de wardriving

Usa Arduino IDE o PlatformIO. El código captura beacons WiFi (SSID, BSSID, RSSI, canal, cifrado), obtiene coordenadas GPS y las escribe en CSV en la SD automáticamente.

`Arduino IDE + ESP32 board manager + TinyGPS++ library`

03 — Sal a mapear tu zona

Conecta la batería, inserta la SD y sal caminando o en coche. El sistema registra automáticamente cada red con GPS. Una caminata de 30 minutos puede capturar cientos de redes en zona urbana.

`~30 redes/minuto en zona urbana densa`

04 — Analiza el mapa en WiGLE o Google Maps

Sube el CSV a WiGLE.net para visualización global, o importa el KML en Google Maps para ver un mapa de calor de tu zona con filtros por seguridad. Identifica negocios y áreas con redes inseguras.

`wigle.net · Google My Maps · QGIS para análisis avanzado`

05 — MARCO LEGAL EN MÉXICO

// IFT · LEY FEDERAL DE TELECOMUNICACIONES · MÉXICO 2026

Reconocimiento pasivo — Legal en modo escucha

El wardriving pasivo — escuchar señales WiFi que se transmiten libremente en el espacio radioeléctrico — es legal en México. Las redes WiFi emiten beacons continuamente de forma pública para anunciar su presencia. El ESP32 en modo pasivo solo recibe esas transmisiones públicas, igual que cualquier celular o laptop cuando busca redes. Lo que está prohibido: conectarse sin autorización, capturar tráfico de datos o intentar romper el cifrado.

// PERSPECTIVA NAVI

El wardriving no ataca redes.
Hace visible lo que ya es público
y nadie se había tomado el tiempo de ver.

$9 USD · ESP32 · GPS · La seguridad WiFi de tu ciudad, en un mapa.