
# Low-Cost Wardriving

**Cristian Trapp Dienst**
trappdienstcristian@hotmail.com

**Mario Martin Sbarbaro**
mmsbarbaro@gmail.com

# Low-cost wardriving

## Aviso de Responsabilidad

Este taller es de carácter educativo.

Todas las prácticas se realizan en entornos controlados y con equipos autorizados.

El uso de las técnicas aprendidas en sistemas ajenos sin permiso es ilegal.

Los instructores y la organización de Ekoparty no se responsabilizan por el uso indebido de la información aquí impartida.

# Low-cost wardriving

## Agenda

- Descripción del Toolset de Exploración Inalámbrica
- Ediciones del Tooltset
- Edición Scout (alta crotera)
- Edición Tracker (tuneada)
- Edición Hunter (full facha)
- Instalación, configuración, prueba e implementación del TS Hunter
- Referencias bibliográficas

# Low-cost wardriving

## Presentación

Lic. **Cristian Trapp Dienst**

Jefe del Departamento de Seguridad Informática del Gobierno de Entre Ríos

Docente/Investigador del LASI de la FCyT UADER

Consultor independiente

# Low-cost wardriving

## Presentación

Lic. **Mario Martin Sbarbaro**

Analista de seguridad del Departamento de Seguridad Informática del Gobierno de Entre Ríos

Docente/Investigador del LASI de la FCyT UADER

Consultor independiente

# Low-cost wardriving

## Descripción del Toolset de Exploración Inalámbrica

El Toolset de Exploración Inalámbrica es un entorno portátil y de bajo costo diseñado para la práctica del wardriving.

# Low-cost wardriving

## Descripción del Toolset de Exploración Inalámbrica ...

A nivel de hardware

Se compone de una Raspberry Pi como unidad central de procesamiento, complementada con placas WiFi USB, un GPS y un power bank que le otorga autonomía en campo.

# Low-cost wardriving

## Descripción del Toolset de Exploración Inalámbrica ...

### A nivel de software

Y sobre esta base de hardware se integra un ecosistema de software libre que incluye Raspberry Pi OS como sistema operativo, gpsd para la gestión de la geolocalización, Kismet como motor de detección y análisis de redes inalámbricas, y SSH para la administración remota. La funcionalidad se completa con scripts propios que automatizan tareas de instalación, captura, control y monitoreo.

# Low-cost wardriving

## Descripción del Toolset de Exploración Inalámbrica ...

En síntesis

La combinación de hardware y de software, transforman al Toolset en una plataforma adaptable tanto para fines de aprendizaje como para proyectos de auditoría y relevamiento de ciberseguridad en redes Wi-Fi.

# Low-cost wardriving

## Ediciones del Toolset

Edición Scout (alta crotera)

Versión liviana, ideal para aprender y explorar redes inalámbricas de forma básica.

Edición Tracker (tuneada)

Versión intermedia, pensada para análisis más detallado con hardware adicional.

Edición Hunter (full facha)

Versión completa, orientada a auditorías y máxima cobertura.

# Low-cost wardriving

## Ediciones del Toolset ...

Desde el punto de vista del hardware

Entre ediciones hay cambios significativos en el hardware y consecuentemente en el costo.

Desde el punto de vista del software

Entre las ediciones existen cambios que simplifican el ecosistema pero el costo no se modifica en ningún caso.

# Low-cost wardriving

## Edición Scout (alta crotera)

Versión liviana, ideal para aprender y explorar redes inalámbricas de forma básica. De costo bajo. Incluye una Raspberry Pi Zero 2 w 64bits, una placa Wi-Fi USB tipo TP-Link TL-WN722n o TP-Link TL-WN422g y un power bank.

# Low-cost wardriving

## Edición Scout (alta crotera) ...

Los materiales necesarios para el Toolset Scout son los siguientes:

(1) Una Raspberry Pi Zero 2 W 64 bits

(1) Un teléfono móvil con GPS y sistema operativo Android

(1) Un placa de red WiFi USB para la banda de los 2.4 GHz

(1) Un power bank

Opcional: (1) Una antena con mayor ganancia para una de las placas WiFi

Programas, aplicaciones y servicios necesarios para llevar a cabo la evaluación utilizando los métodos Wardriving, Warbiking y Warwalking.

# Low-cost wardriving

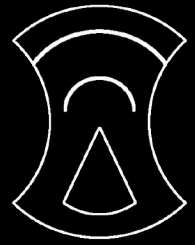
## Edición Scout (alta crotera) ...

# Low-cost wardriving

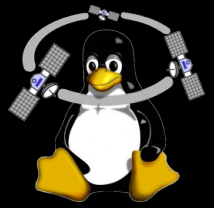
## Edición Scout (alta crotera) ...

**App NetShare**


Script **install_tss.sh**
Script **config_wifi_tss.sh**
Script **menu_tss.sh**



**Kismet**

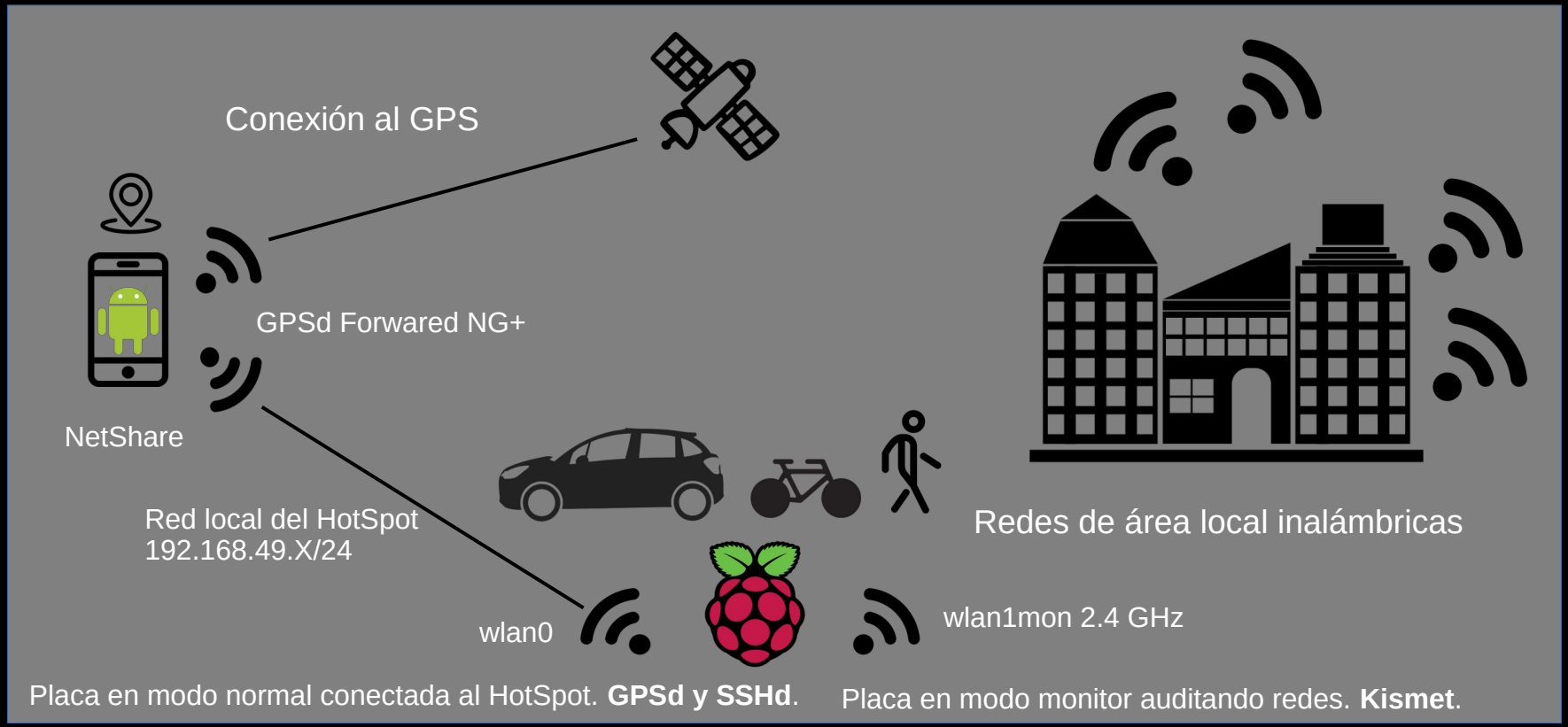


**GPSd**

**App GPSd Forwared NG+**

# Low-cost wardriving

## Edición Scout (alta crotera) ...



# Low-cost wardriving

## Edición Tracker (tuneada)

Versión intermedia, pensada para análisis más detallado con hardware adicional. De costo Medio. Incluye Raspberry Pi 3B+, una placa Wi-Fi USB tipo TP-Link TL-WN722n o TP-Link TL-WN422g, una placa Wi-Fi USB TP-Link T2U plus y un power bank.

Versión intermedia ALTERNATIVA,  incluye raspberry pi zero 2 w 64bits, una placa Wi-Fi USB TP-Link T2U plus y un power bank.

# Low-cost wardriving

## Edición Tracker (tuneada) ...

Los materiales necesarios para el Toolset Tracker son los siguientes:

(1) Una Raspberry Pi 3 Model B+

(1) Un teléfono móvil con GPS y sistema operativo Android

(1) Un placa de red WiFi USB para la banda de los 2.4 GHz

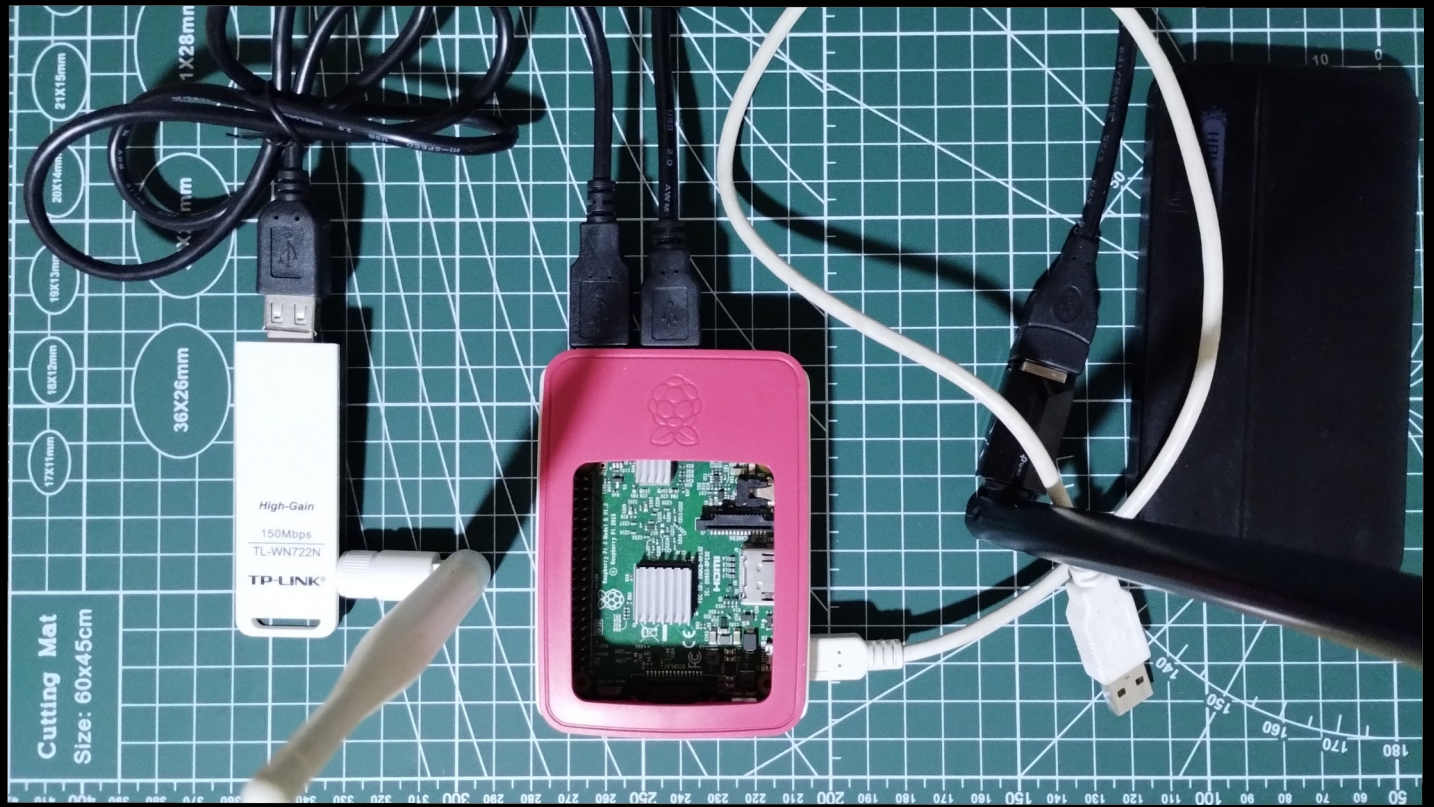
(1) Un placa de red WiFi USB para la banda de los 5 GHz

(1) Un power bank

Programas, aplicaciones y servicios necesarios para llevar a cabo la evaluación utilizando los métodos Wardriving, Warbiking y Warwalking.

# Low-cost wardriving

## Edición Tracker (tuneada) ...

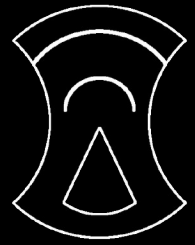


# Low-cost wardriving

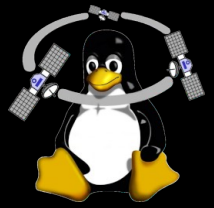
## Edición Tracker (tuneada) ...

**App NetShare**


Script **install_tst.sh**
Script **config_wifi_tst.sh**
Script **menu_tst.sh**



**Kismet**

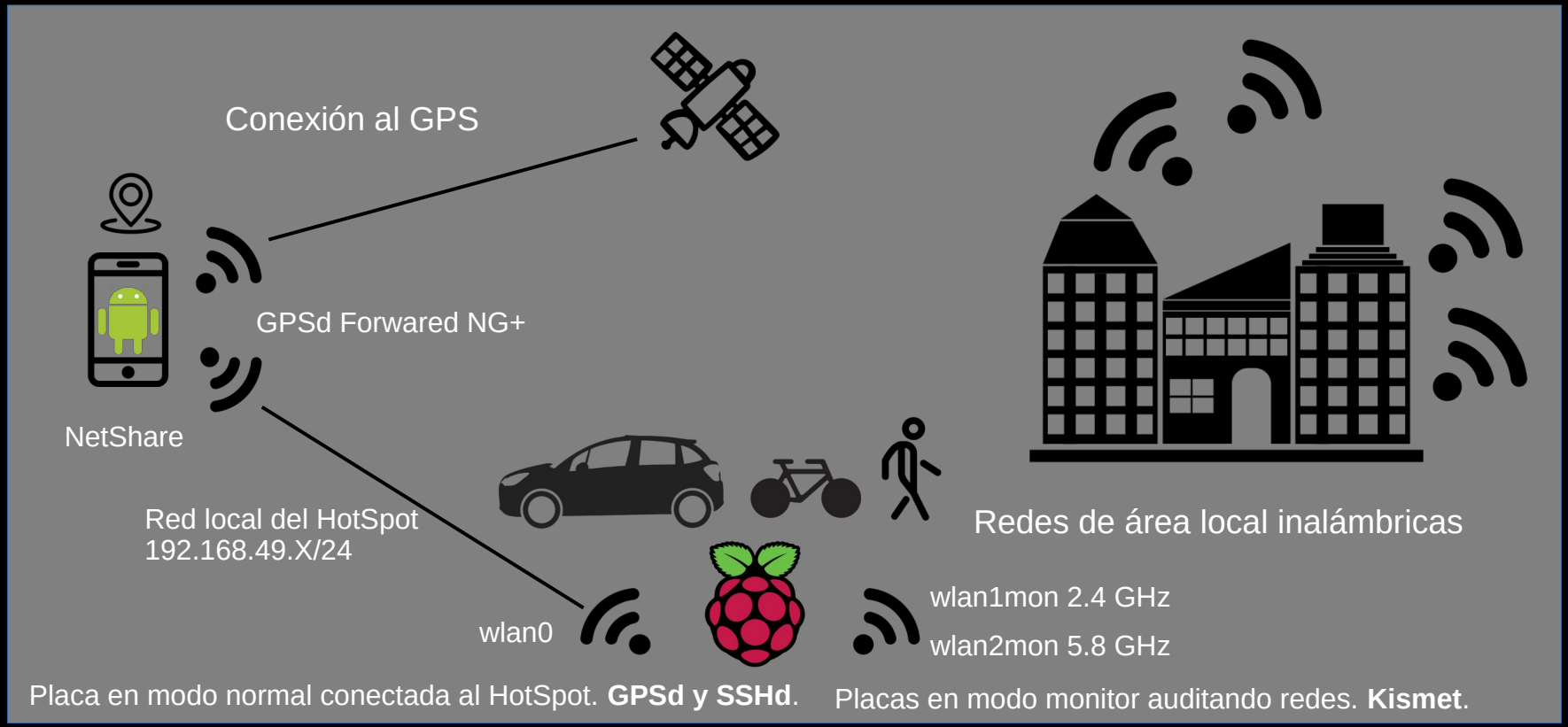


**GPSd**

**App GPSd Forwared NG+**

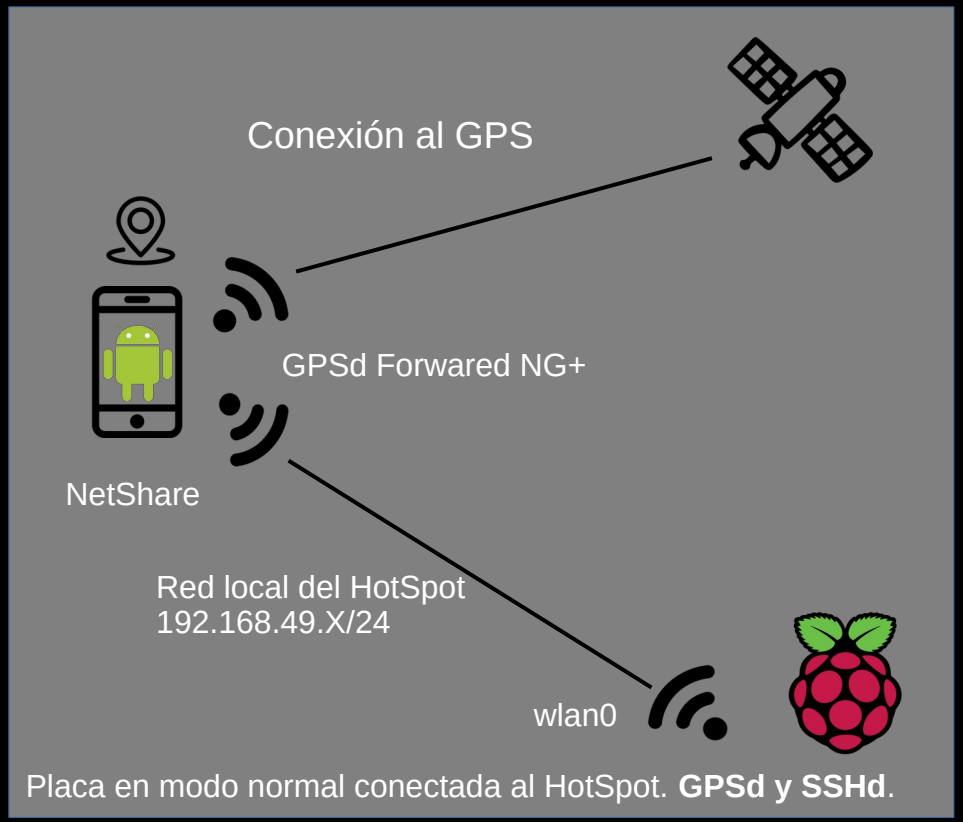
# Low-cost wardriving

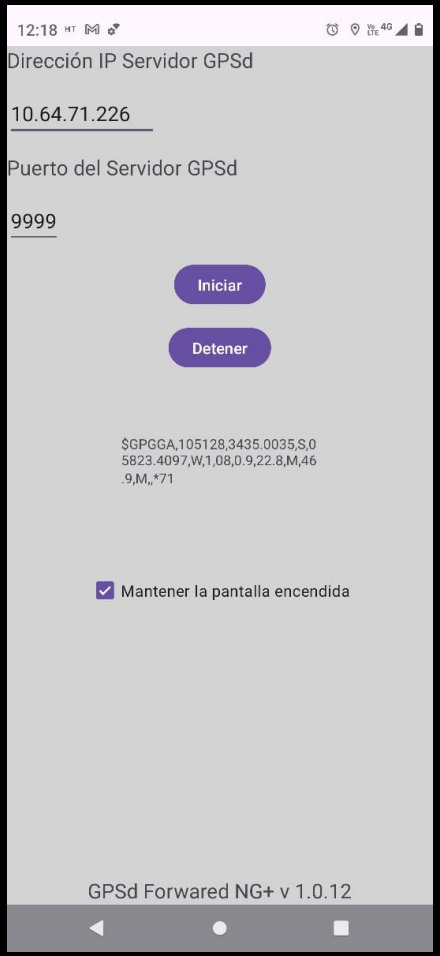
## Edición Tracker (tuneada) ...



# Low-cost wardriving

## Edición Tracker (tuneada) ...



# Low-cost wardriving

## Edición Hunter (full facha)

Versión completa, orientada a auditorías y máxima cobertura. De costo Alto. Incluye raspberry pi 3B+, una  placa Wi-Fi USB tipo TP-Link TL-WN722n, una placa Wi-Fi USB TP-Link T2U plus, una placa Wi-Fi USB tipo TP-Link TL-WN7200ND,  un GPS USB y un power bank.

# Low-cost wardriving

## Edición Hunter (full facha) ...

Los materiales necesarios para el Toolset Hunter son los siguientes:

(1) Una Raspberry Pi 3 Model B+

(1) Un teléfono móvil con sistema operativo Android

(2) Dos placas de red WiFi USB para la banda de los 2.4 GHz

(1) Un placa de red WiFi USB para la banda de los 5 GHz

(1) Un GPS USB

(1) Un power bank

Programas, aplicaciones y servicios necesarios para llevar a cabo la evaluación utilizando los métodos War-X.

# Low-cost wardriving

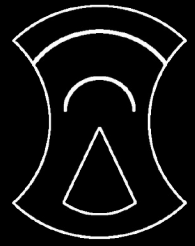
## Edición Hunter (full facha) ...

# Low-cost wardriving

## Edición Hunter (full facha) ...

**Zona Wi-Fi**

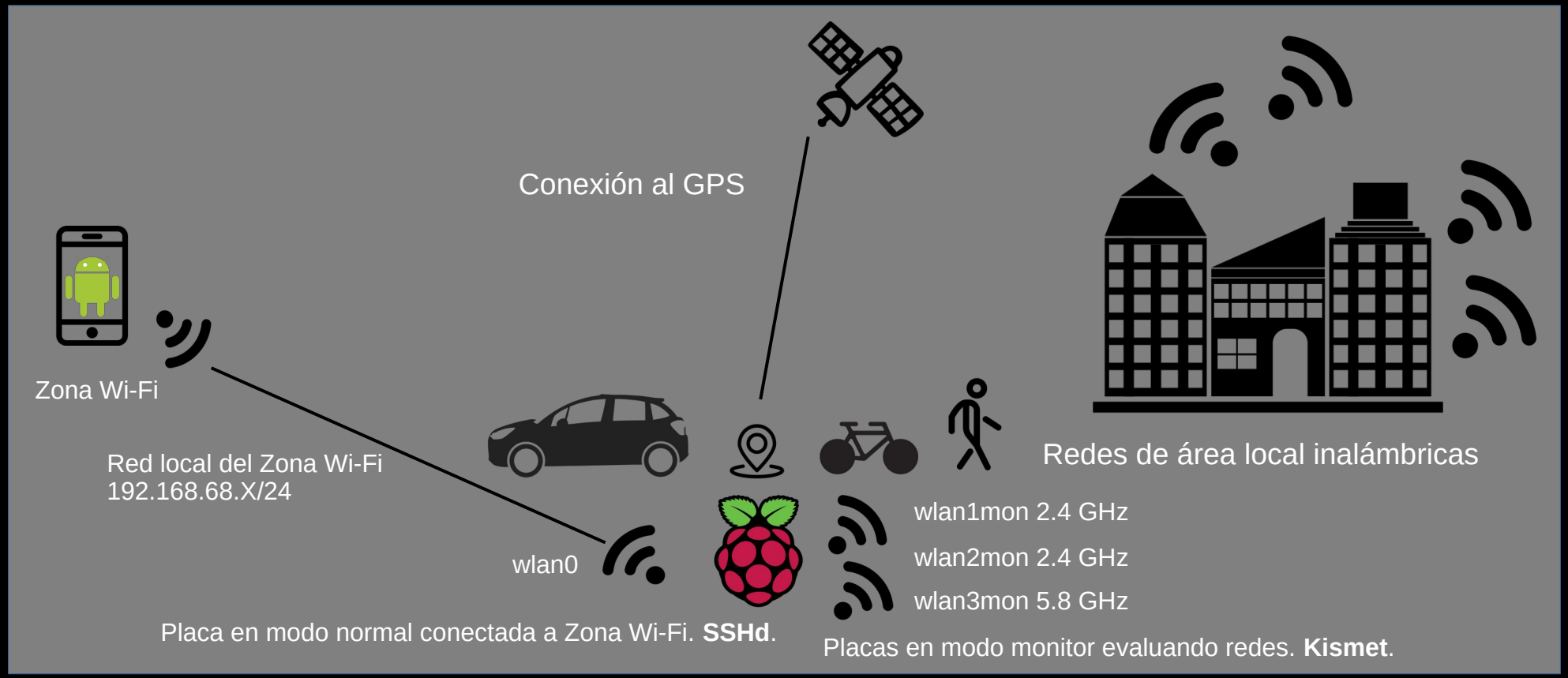

Script **install_tsh.sh**
Script **config_wifi.sh**
Script **menu_tsh.sh**
Script **WifiUserPassWPSDefault.sh**



**Kismet**

# Low-cost wardriving

## Edición Hunter (full facha) ...



# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH

- Configuración de Raspberry Pi OS.
- Crear script para configurar interfaces de red (config_wifi_tsh.sh).
- Crear script para probar redes Wi-Fi con configuración por defecto.
- Configurar ssh (opcional).
- Instalar y configurar kismet.
- Modificar el inicio del arranque de Raspberry Pi OS en el rc.local.
- Crear y configurar usuarios de raspbian para los comandos (comenzar, detener, reiniciar, reboot, apagar y ver el estado).

# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

## Configuración de Raspberry Pi OS

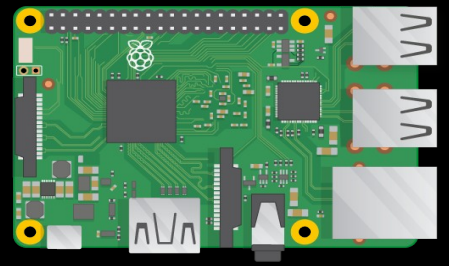
### Configuración de Raspberry Pi OS desde la consola

Ejecutar el comando *sudo raspi-config*.

```
┤ Raspberry Pi Software Configuration Tool (raspi-config) ├

1 Change User Password  Change password for the default user (pi)
2 Hostname              Set the visible name for this Pi on a network
3 Boot Options          Configure options for start-up
4 Localisation Options  Set up language and regional settings to match your location
5 Interfacing Options   Configure connections to peripherals
6 Overclock             Configure overclocking for your Pi
7 Advanced Options      Configure advanced settings
8 Update                Update this tool to the latest version
9 About raspi-config    Information about this configuration tool

                <Select>                                <Finish>
```



# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

Crear script para configurar interfaces de red (config_wifi_tsh.sh)

config_wifi_tsh.sh

Ver  configuración

```
#!/bin/bash
# Direcciones MAC a las que les queremos asignar un nombre
declare -A mac_to_name
mac_to_name["14:cc:20:26:af:4e"]="wifi24"
mac_to_name["ec:75:0c:42:b1:6b"]="wifi58"
mac_to_name["18:a6:f7:0d:d7:72"]="wificonnect"
# Obtener la lista de interfaces wlanX
for interface in $(ip link show | grep -oP 'wlan\d' | sort | uniq); do
...
```

# Low-cost wardriving

Instalación, configuración, prueba e implementación TSH ...

Crear script para probar redes Wi-Fi con configuración por defecto

WifiUserPassWPSDefault.sh

```
#/bin/bash
INTERVALO=5
INTERFACE=$1
function IntentoConexion(){
    ssid=$1
    clave=$2
    macaddress=$3
    Interface=$4
...
```

Ver  configuración

# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

### Configurar ssh (opcional)

Configurar el servicio ssh

*# vi /etc/ssh/sshd_config*

*PermitRootLogin no # No permitir login directo de root*
*X11Forwarding no # Desactivar reenvíos innecesarios*
*AllowTcpForwarding no # Desactivar reenvíos innecesarios*
*PermitTunnel no # Desactivar reenvíos innecesarios*
*MaxAuthTries 3 # Limitar intentos*
*LoginGraceTime 30 # Aplicar desconexión rápida*

# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

### Instalar y configurar kismet

Instalar kismet

```
# apt update

# apt upgrade -y

# apt install -y git build-essential libmicrohttpd-dev libnl-3-dev \
 libnl-genl-3-dev libcap-dev libpcap-dev pkg-config zlib1g-dev \
 libncurses5-dev libnm-dev libdw-dev libsqlite3-dev libprotobuf-dev \
 libprotobuf-c-dev protobuf-compiler protobuf-c-compiler \
 libsensors4-dev libusb-1.0-0-dev libwebsockets-dev python3 \
 python3-protobuf python3-requests python3-numpy
```

# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

### Instalar y configurar kismet ...

Instalar kismet

```
# echo "deb http://www.kismetwireless.net/repos/apt/release/bookworm \
 bookworm main" | sudo tee /etc/apt/sources.list.d/kismet.list

# wget -O - https://www.kismetwireless.net/repos/kismet-release.gpg.key \
| apt-key add -

# apt update

# apt install -y kismet

# kismet --version
```

# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

### Instalar y configurar kismet ...

Configurar kismet

*# vi /etc/kismet/kismet_site.conf*

*gps=serial:device=/dev/ttyACM0,name=ttyACM0,reconnect=true,baud=9600*

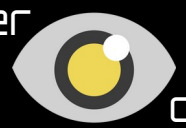
*source=wifi24:name=wifi24,interface=wifi24,type=linuxwifi*

*source=wifi58:name=wifi58,interface=wifi58,type=linuxwifi*

*# vi /etc/kismet/kismet_logging.conf*

Establecer la siguiente configuración:

log_prefix=/home/tsh/kismet



# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

### Modificar el inicio del arranque de Raspberry Pi OS tocando el rc.local

Modificar el archivo rc.local

*#vi /etc/rc.local*

Agregar al final del archivo las siguientes líneas:

*bash /home/tsh/config_wifi_tsh.sh*

*kismet –log-debug 2>&1 -t "Kismet_$(date +'%d-%m-%Y_%H-%M-%S')" &*

*bash /home/tsh/WifiUserPassWPSDefault.sh wificonnect | tee -a /home/tsh/WifiUserPassWPSDefault.log*


configuración

# Low-cost wardriving

Instalación, configuración, prueba e implementación TSH ...

Crear y configurar usuarios de Raspberry Pi OS para los comandos

Comando comenzar

*# adduser comenzar*

*# vi /home/comenzar/.bashrc*

Agregar las siguientes líneas al final del archivo

*sudo kismet –log-debug 2>&1 -t "Kismet_$(date +'%d-%m-%Y_%H-%M-%S')" &*

# Low-cost wardriving

Instalación, configuración, prueba e implementación TSH ...

Crear y configurar usuarios de Raspberry Pi OS para los comandos

> Comando detener
>
> *# adduser detener*
>
> *# vi /home/detener/.bashrc*
>
> Agregar las siguientes líneas al final del archivo
>
> *sudo pkill kismet*

# Low-cost wardriving

Instalación, configuración, prueba e implementación TSH ...

Crear y configurar usuarios de Raspberry Pi OS para los comandos

## Comando reiniciar

*# adduser reiniciar*

*# vi /home/reiniciar/.bashrc*

Agregar las siguientes líneas al final del archivo

*sudo pkill kismet*

*sudo pkill -f WifiUserPassWPSDefault*

*echo "Reiniciando kismet y WifiUserPassWPSDefault.sh ..."*

*sleep 10*

*sudo bash /home/tsh/WifiUserPassWPSDefault.sh wificonnect | tee -a ...*

*sudo kismet –log-debug 2>&1 -t "Kismet_$(date +'%d-%m-%Y_%H-%M-%S')" &*

# Low-cost wardriving

Instalación, configuración, prueba e implementación TSH ...

Crear y configurar usuarios de Raspberry Pi OS para los comandos

## Comando estado

```
# adduser estado
# vi /home/estado/.bashrc
```

Agregar las siguientes líneas al final del archivo

```
If pidof kismet > /dev/null
then
        echo "Kismet está en ejecución"
else
        echo "Kismet no se está ejecutando"
fi
...
```

# Low-cost wardriving

Instalación, configuración, prueba e implementación TSH ...

Crear y configurar usuarios de Raspberry Pi OS para los comandos

## Comando reboot

*# adduser reboot*

*# vi /home/reboot/.bashrc*

Agregar las siguientes líneas al final del archivo

```
if pidof kismet then
        sudo pkill kismet
fi
sudo reboot
```


configuración

# Low-cost wardriving

Instalación, configuración, prueba e implementación TSH ...

Crear y configurar usuarios de Raspberry Pi OS para los comandos

Comando apagar

```
# adduser apagar
# vi /home/apagar/.bashrc
```

Agregar las siguientes líneas al final del archivo

```
If pidof kismet then
        sudo pkill kismet
fi
sudo shutdown now
```

Ver  configuración

# Low-cost wardriving

## Instalación, configuración, prueba e implementación TSH ...

### Script de instalación y menú de gestión de TSH

Script install_tsh.sh


```
#!/bin/bash
echo "------------------------------------------------------"
echo "Instalando el ToolSet Wardriving Hunter en Raspberry Pi OS ..."
echo "------------------------------------------------------"
# Creación de una clave para los usuarios de sistema
LENGTH=8
PASSWORD=$(tr -dc 'A-Za-z0-9' </dev/urandom | head -c "$LENGTH")
echo "$PASSWORD" > /root/users_passwords.txt
...
```

# Low-cost wardriving

**https://github.com/seguridaddgin/toolset-wardriving**

# ¡Muchas Gracias!

Y nos vemos en el trencito hacker de la alegría

# Low-cost wardriving

## Referencias bibliográficas (libros)


- Huidobro, J. M. y Luque, J. (2014). *Comunicaciones por radio. Tecnologías, redes y Servicios de Radiocomuniaciones. El especto Electromagnético* (1ra. ed.). México: Alfaomega.
- Stallings, W. (2004). *Fundamentos de seguridad en redes. Aplicaciones y estándares* (2da. ed.). Madrid: Pearson Educación.
- Tanenbaum, A. S. y Wetherall, D. J. (2012). *Redes de Computadoras* (5ta. ed.). México: Pearson Educación.


# Low-cost wardriving

## Referencias bibliográficas (artículos científicos) ...


- Díaz, J., Robles, M., Venosa, P., Macia, N. y Vodopivec, G. (Octubre, 2008). Wardriving: an experience in the city of La Plata. Trabajo presentado en el XIV Congreso Argentino de Ciencias de la Computación, Bueno Aires. Recuperado de: http://sedici.unlp.edu.ar/handle/10915/21678.

- Millán, A. F., Daza, R. y Campiño, J. (2006). Estudio de los puntos de acceso inalámbricos 802.11 en la ciudad de Cali usando las técnicas WAR-X. SISTEMAS & TELEMÁTICA, 4(7), 35-42.

- GONZÁLEZ MARRÓN, D., PÉREZ HERNÁNDEZ, I., MARQUÉZ CALLEJAS, A. y BADILLO PAREDES, L. (2017). Análisis de vulnerabilidades en redes inalámbricas instaladas en diversos municipios del Estado de Hidalgo. Revista de Tecnología Informática, 1(2), 32-40.


# Low-cost wardriving

## Referencias bibliográficas (ponencias) ...


- SBARBARO, M. M.,TRAPP DIENST, C. A., DOBLER, B. J., BRIGANTI BARRET, M. A., PASUTTI, T., CHAVES, E. M. y LÓPEZ, F. (Agosto, 2024). Seguridad inalámbrica en el casco cívico de la ciudad de Paraná. Trabajo presentado en la Primera Jornada de Ciencia y Tecnología, Paraná. Recuperado de: https://fcyt.uader.edu.ar/wp-content/uploads/2025/08/LIBRO-DE-RESUMENES-2024.pdf.