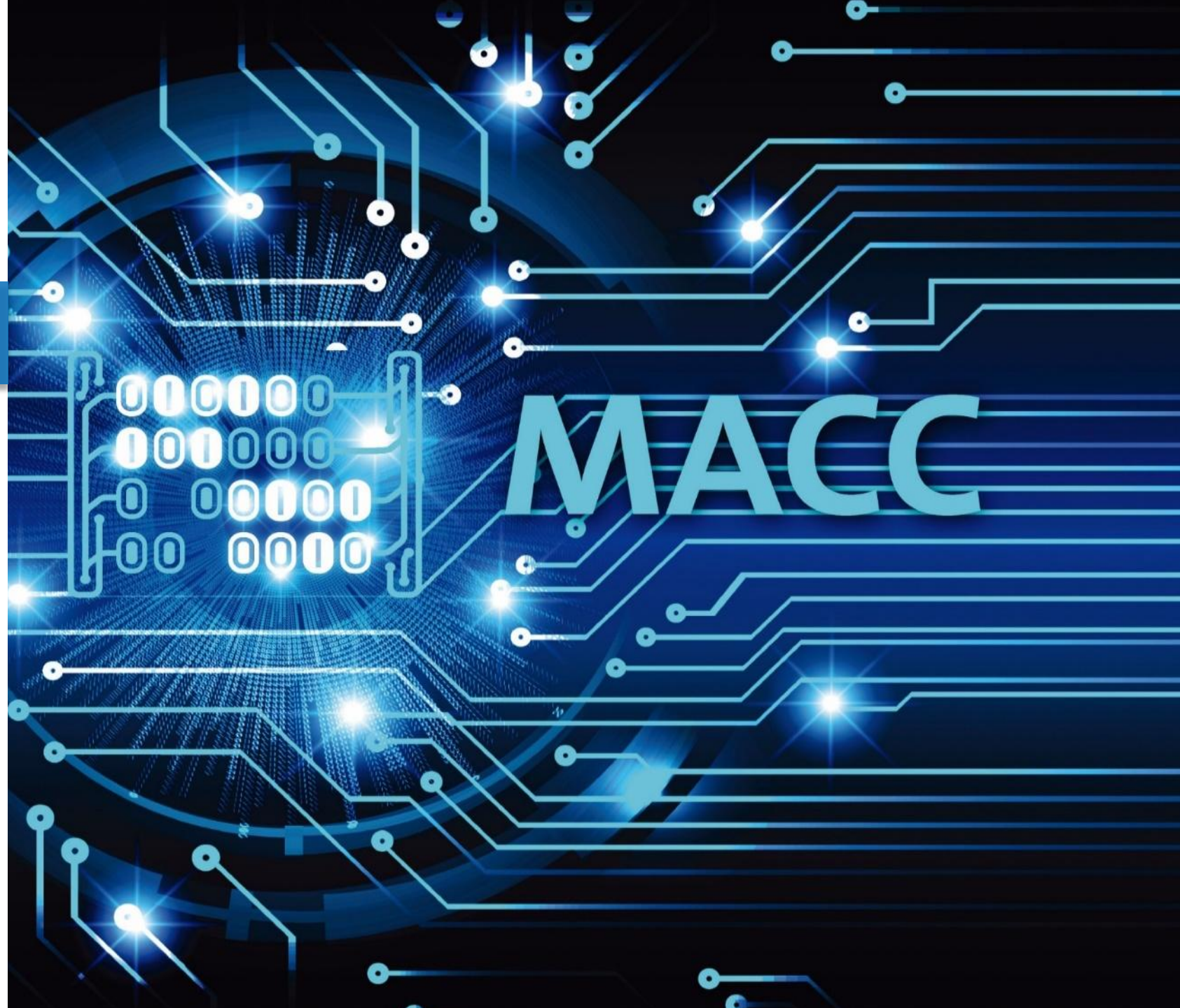
Universidad del Rosario

MACC
Matemáticas Aplicadas y Ciencias de la Computación

Wireless Networks

Hacking Ético



Daniel Orlando Díaz López, PhD

Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co

Service Set Identifier (SSID): Identificador único de hasta 32 caracteres alfanuméricos dado a una red WLAN (Wireless Lan Access Network)

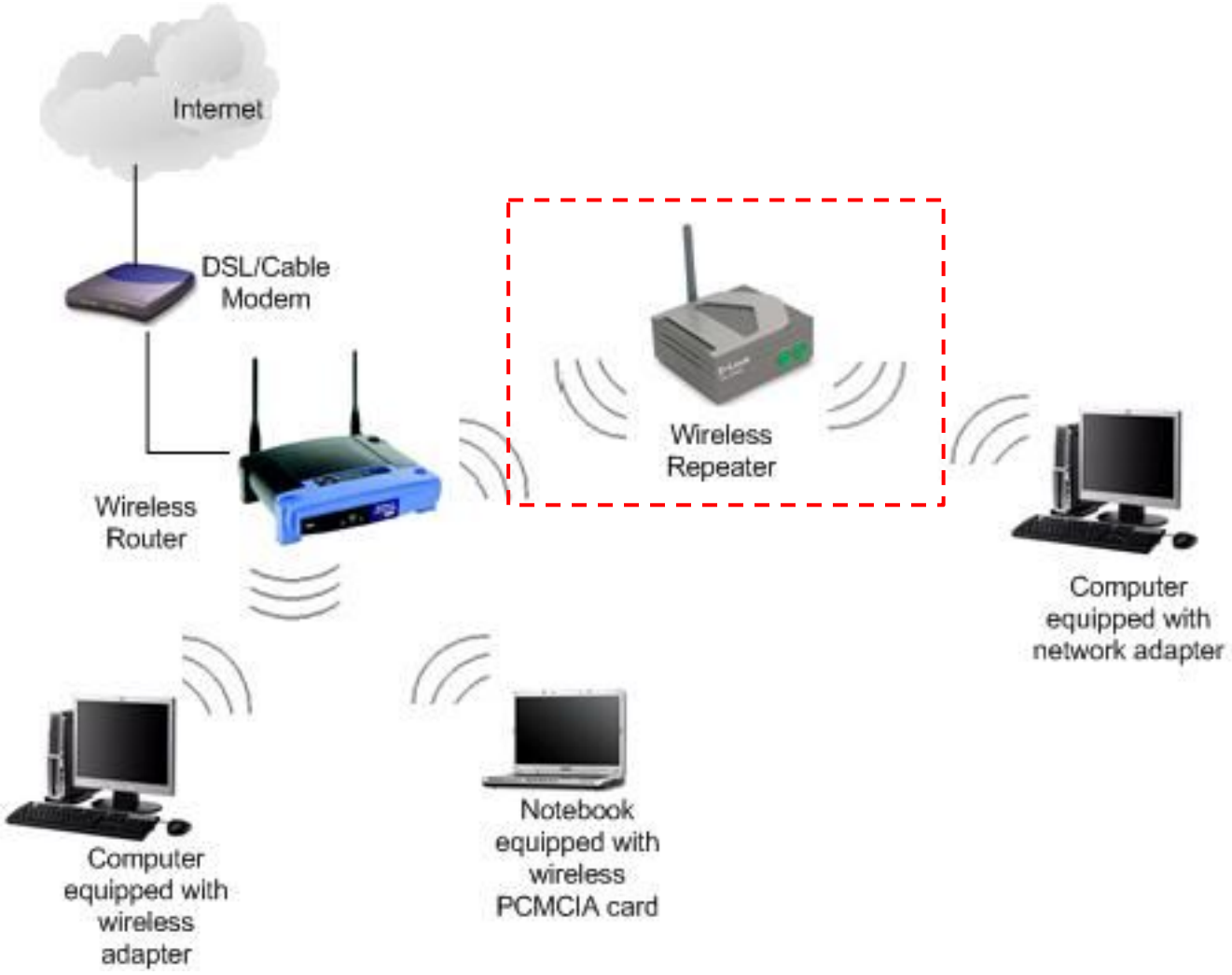
BSSID: Es la dirección MAC de un Access Point / Router inalámbrico

Access Point: Elemento de red que conecta dispositivos clientes a una red inalámbrica

Bandwidth (Ancho de Banda): Representa la cantidad de información que puede ser transmitida por una red inalámbrica

Hotspot: lugar en el cual se dispone de servicio de red inalámbrica

1. Repetidor para extender el hotspot en el cual opera un SSID

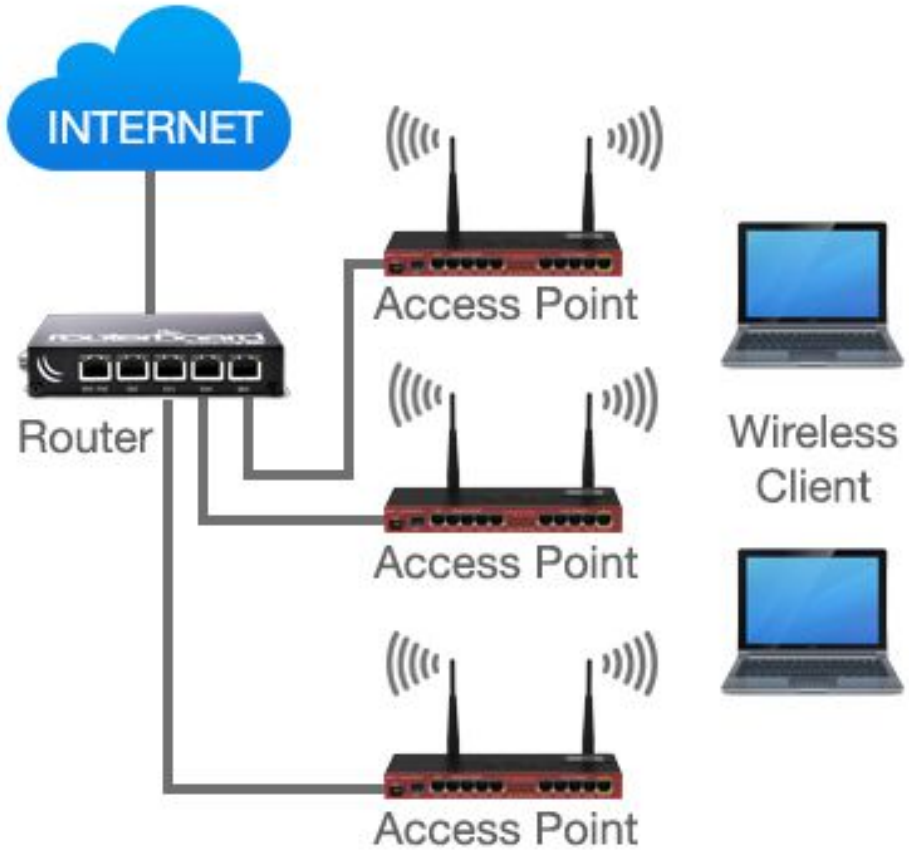


But it here!

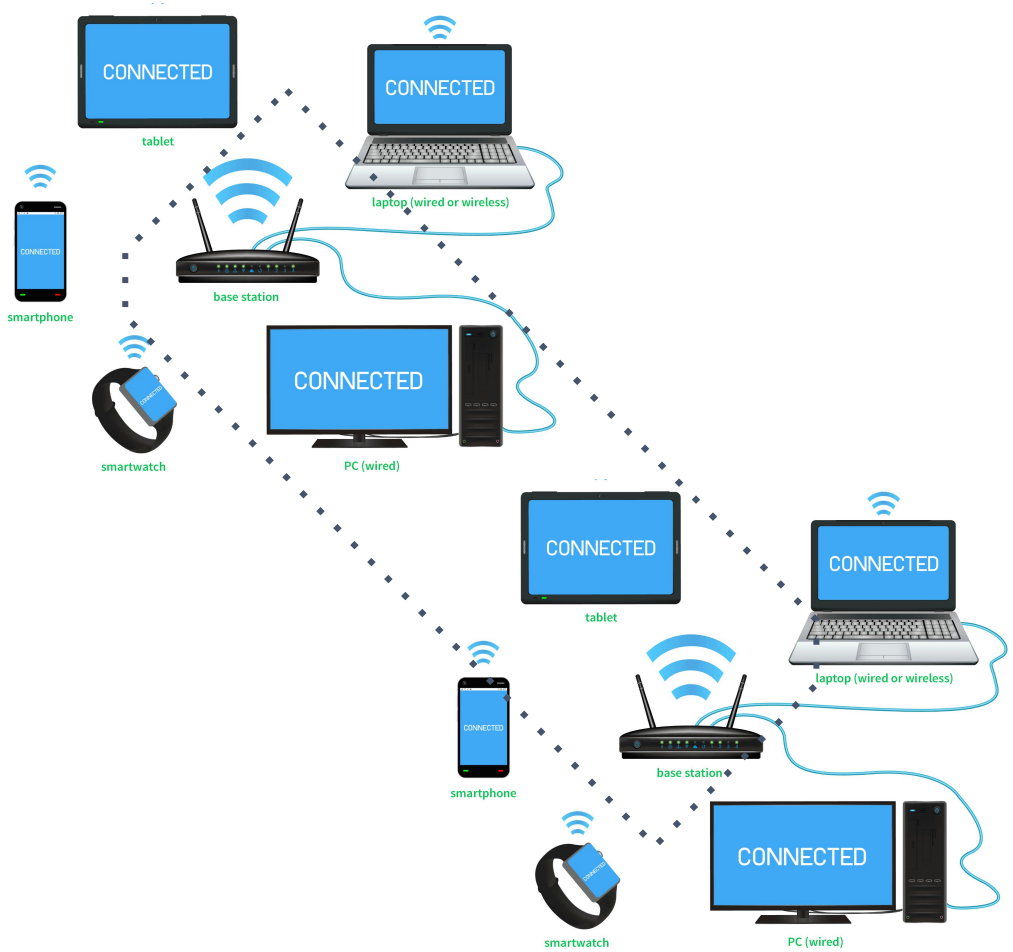
Tipos de conexiones inalámbricas

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

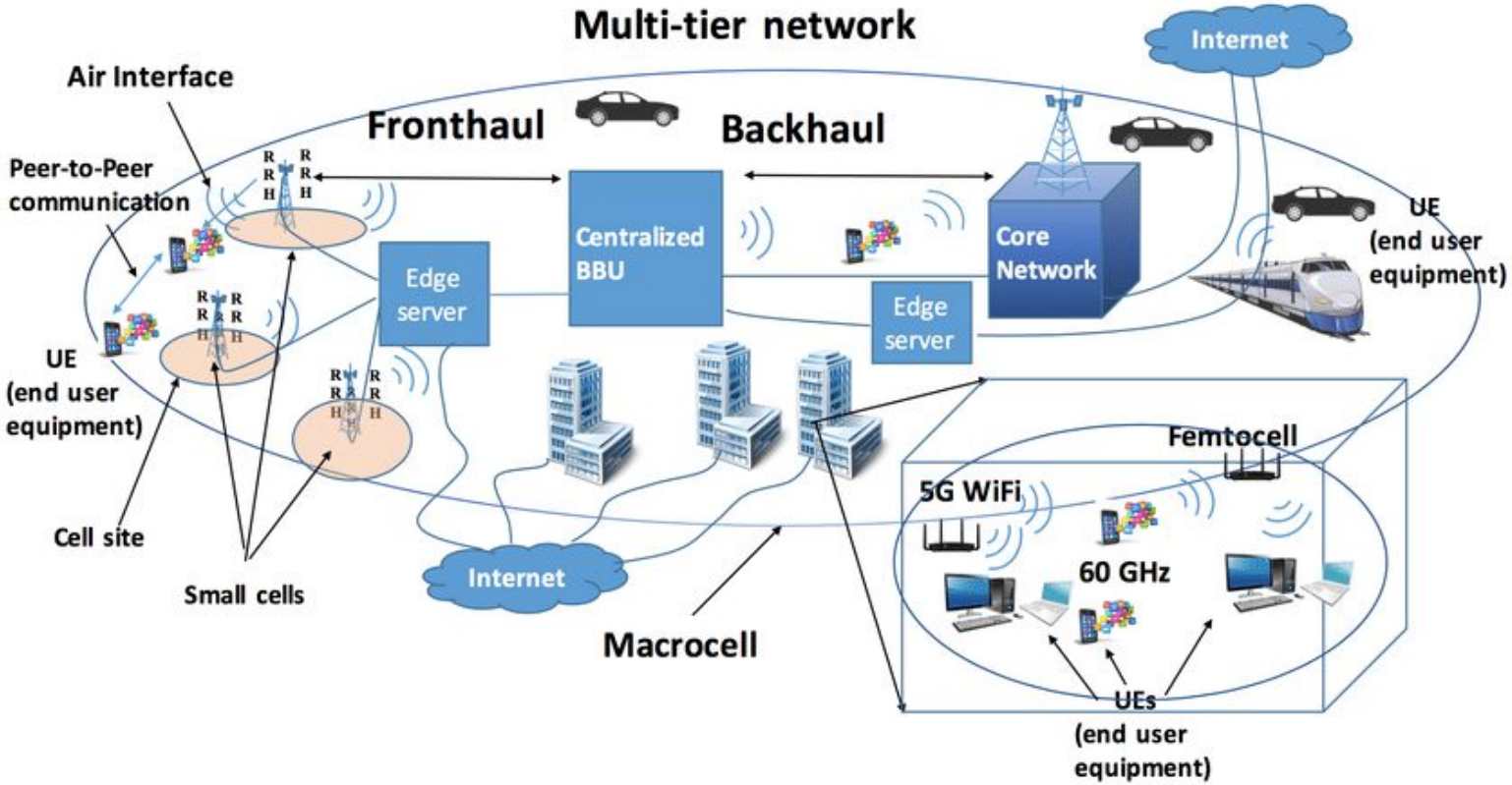
2. Múltiples APs desplegados y sirviendo el mismo SSID



3. 2 o más APs, cada uno perteneciendo a una red distinta (SSID diferente), Y conectados inalámbricamente



4. Redes de telefonía móvil



Modem 4G

Buy it here!

	ZigBee and 802.15.4	GSM/GPRS CDMA	802.11	Bluetooth
Focus Application	Monitoring and Control	Wide Area Voice and Data	High-Speed Internet	Device Connectivity
Battery Life	Years	1 Week	1 Week	1 Week
Bandwidth	250 Kbps	Up to 2 Mbps	Up to 54 Mbps	720 Kbps
Typical Range	100+ Meters	Several Kilometers	50-100 Meters	10-100 Meters
Advantages	Low Power, Cost	Existing Infrastructure	Speed, Ubiquity	Convenience

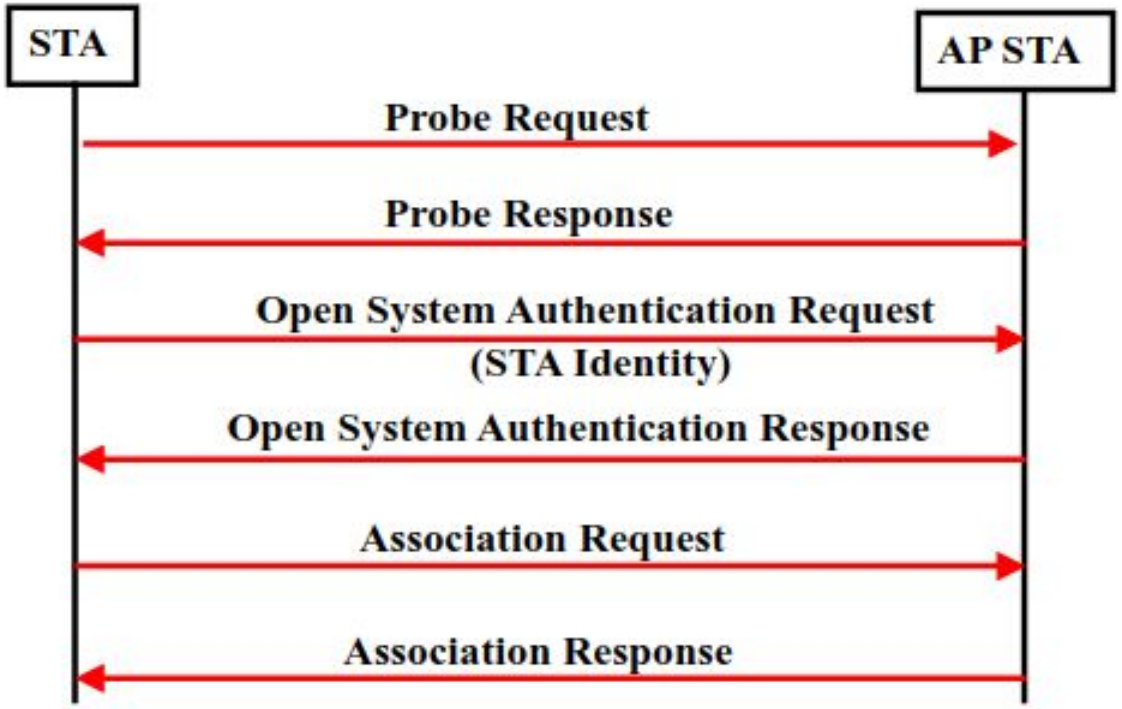
Bandwidth vs Range
Battery life vs Bandwidth

Wifi Authentication Modes

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

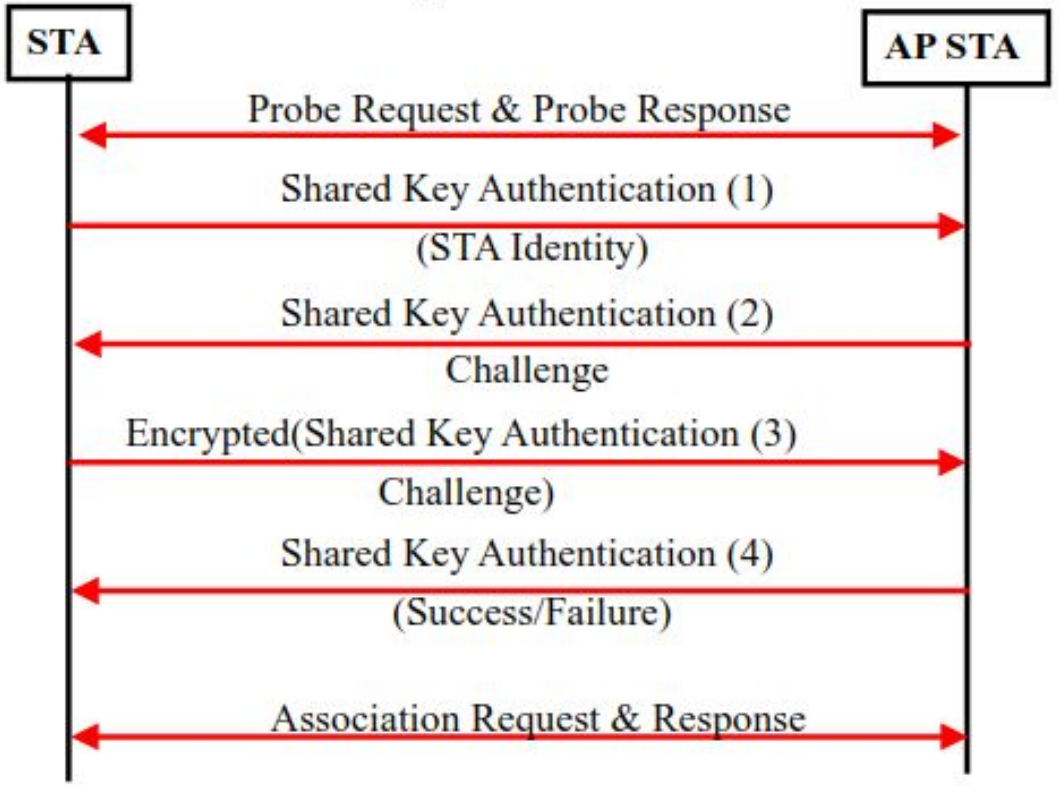
Redes con autenticación abierta

Ejemplos: Restaurantes, Aeropuertos, puntos Vive Digital, etc



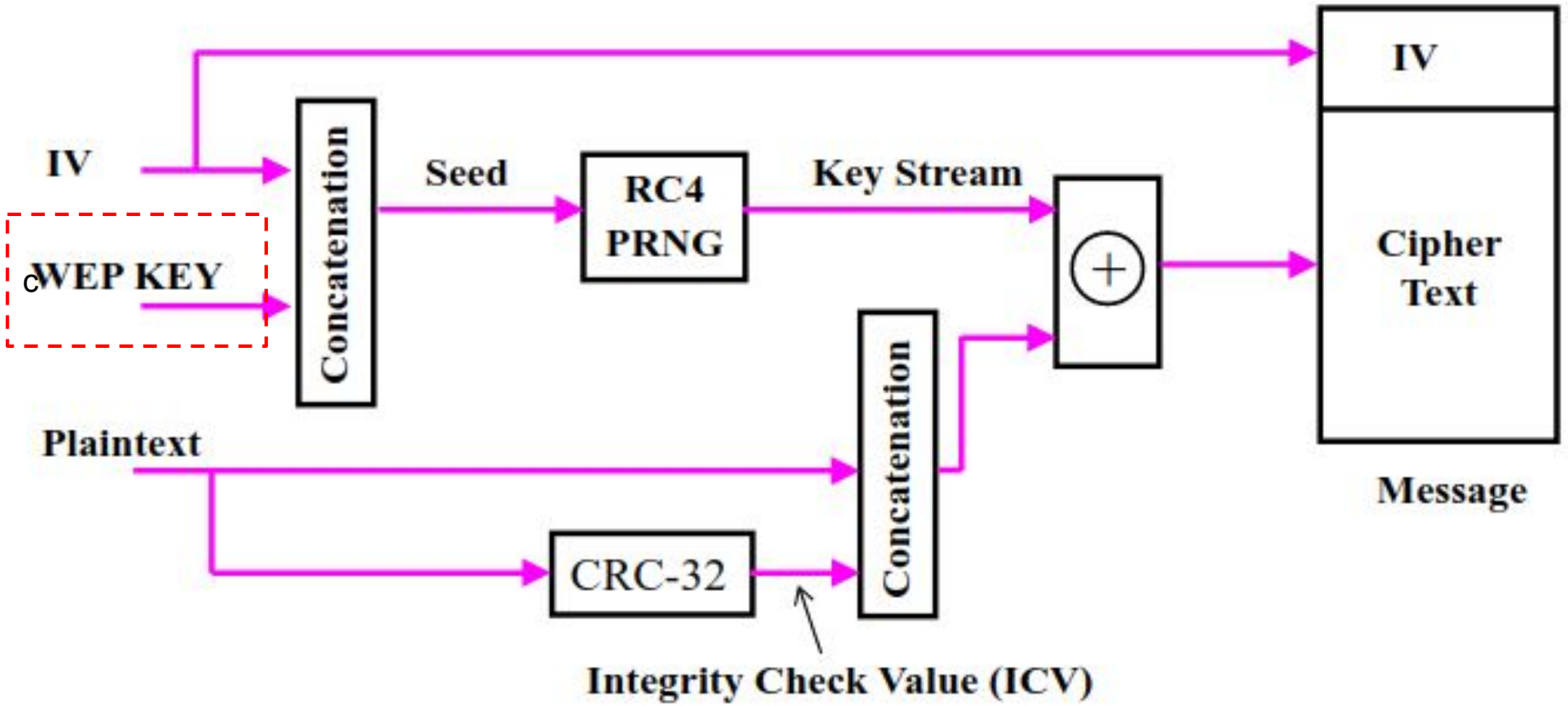
Redes con autenticación de llave compartida tipo WEP

Ejemplos: Red inalámbrica de hogar, algunas oficinas, etc



WEP (Wired Equivalent Privacy) utiliza el algoritmo de cifrado RC4

Contraseña de una red inalámbrica de tipo WEP



Problemas de WEP (Wired Equivalent Privacy)

- El vector de inicialización es de solo 24 bits: Esto implica que en algún punto se repetirá el mismo vector de inicialización para el cifrado de datos, provocando una colisión
- Se puede hacer un ataque estadístico capturando varios paquetes cifrados por WEP y determinando la llave
- El validador de integridad CRC-32 puede ser manipulado para producir un ICV válido para un mensaje falso

Wifi Authentication Modes

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

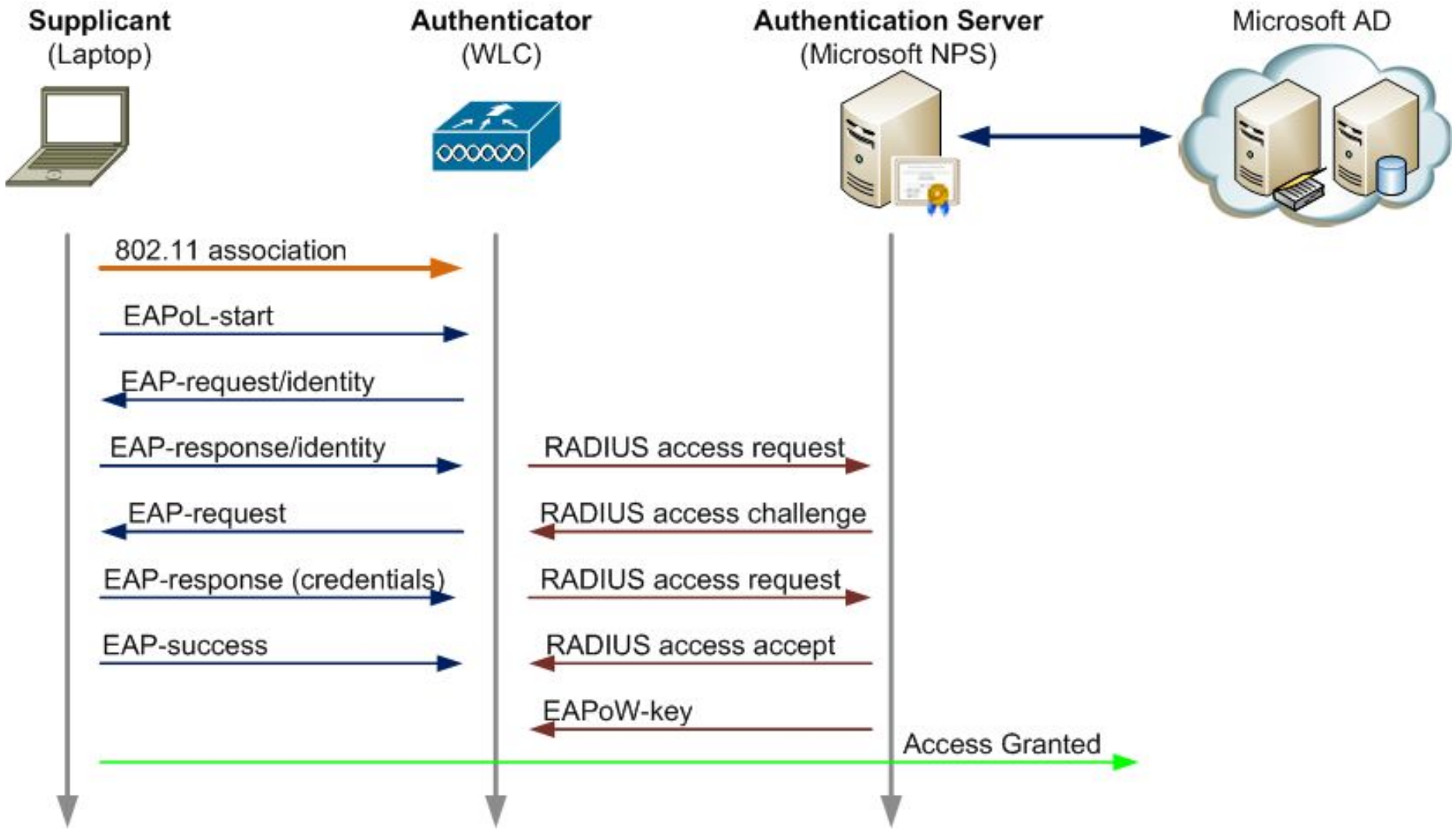
	WEP	WPA	WPA2
The main Purpose	Security is provided in contrast to wired networks	Implementation of major IEEE802.11i standards with WEP without requiring new hardware	Complete IEEE 802.11i standards are implemented with new enhancements of WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Authentication is provided through chipper blocks with CCMP and AES.
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Data integrity is provided through Message Integrity Code.	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Key management is not provided	The 4 way handshaking mechanism is used to provide for key management	The 4 way handshaking mechanism is used to provide for key management
Compatibility in terms of Hardware	Possible to deploy on current hardware infrastructure	Possible to deploy on both current and previous hardware	Older Network Interface Cards are not supported. Only the 2006 and newer.
Vulnerability	Vulnerable against Chopchop, Bittau's fragmentation and DoS attacks including variety of DoS attacks.	Vulnerable against Chopchop, Ohigashi-Morii, WPA-PSK, and Dos attacks.	Vulnerable against DoS attacks due to unprotected control frames and MAC spoofing
Deployment in terms of complexity	Easy to deploy and configure		WPA-2 requires complicated setup with WPA enterprise.
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	Implementation of 48-bit datagram/packet number protects against replay attack

¡WEP fue reemplazado por WPA y después por WPA2!

Wifi Authentication Modes

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Autenticación utilizando un servidor de autenticación



Tipos de ataques a redes inalámbricas

Network Layer	Security Attack	Countermeasure
Physical	Jamming	Spread-spectrum, frequency hopping
	Tampering	Tamper-proof design
Link	Collisions	Error-correcting codes
	Exhaustion	Data rate limits, time division multiplexing
	Unfairness	Short frames
Network and Routing	Spoofing, altering, replaying	Authentication, link-layer encryption
	Sinkholes	Authentication, link-layer encryption
	Wormholes	Authentication, geographic routing, tight synchronisation
	Sybil	Authentication, public key cryptography
	Selective forwarding	Authentication, link-layer encryption, multipath routing
	HELLO attack	Authentication, bidirectional link and identity verification
	Acknowledge spoofing	Authentication
Transport	Flooding	Client puzzles, authenticated broadcast
	Desynchronization	Authentication
Application	Stimuli attack	Authentication
	Packet injection	Authentication

Realizar diferentes tipos de ataques a una red inalámbrica

Laboratorio

1. Iniciar una máquina Kali Linux en modo Live CD
2. Realizar reconocimiento de las redes inalámbricas del entorno

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Realizar diferentes tipos de ataques a una red inalámbrica

1. Descargar la última versión de Kali linux en formato ISO

kali.org/downloads/

KALI BY OFFENSIVE SECURITY

Blog Downloads Training Documentation

concurrent connections.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 32-Bit	Torrent	2019.3	2.9G	3fdf8732df5f2e935e3f21be93565a113be14b4a8eb410522df60e1c4881b9a0
Kali Linux 64-Bit	Torrent	2019.3	2.9G	d9bc23ad1ed2af7f0170dc6d15aec58be2f1a0a5be6751ce067654b753ef7020
Kali Linux Large 64-Bit	Torrent	2019.3	3.5G	dd44391927d38d91cae96ed1a8b918767d38bee2617761fab2d54ad8c77319ec

Today

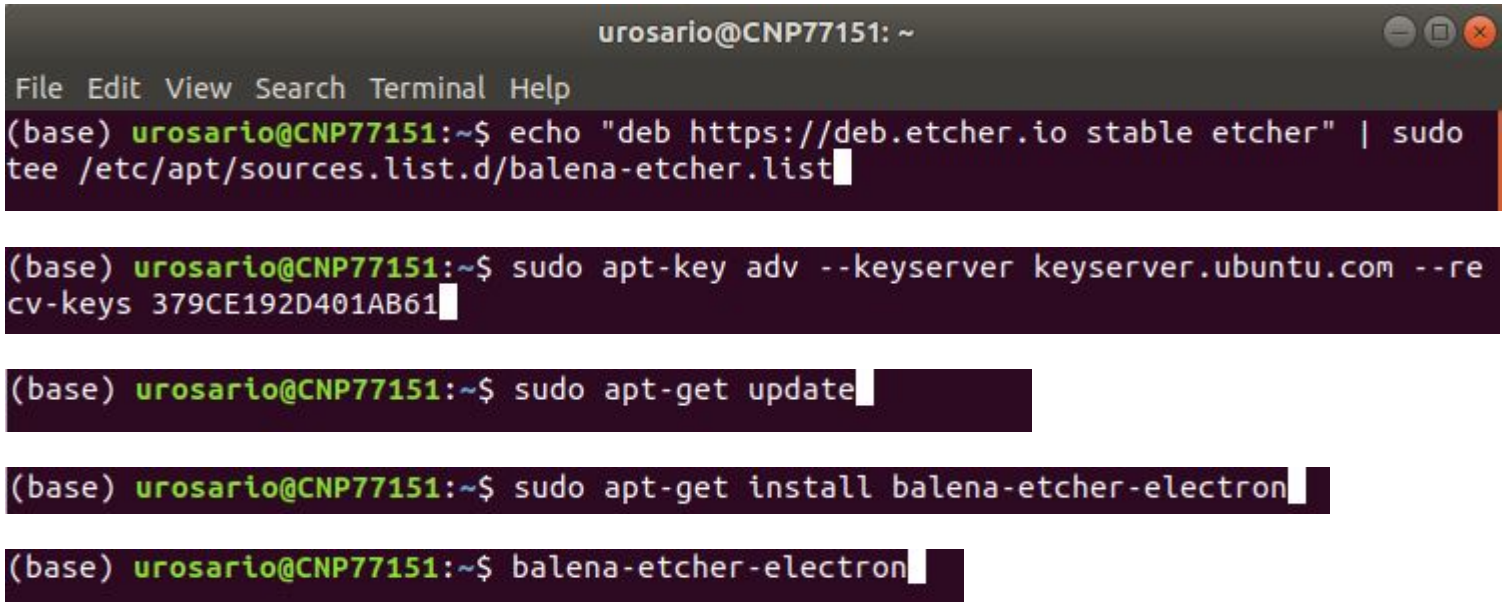
kali-linux-2019.3-amd64.iso

http://kali.download/kali-images/kali-2

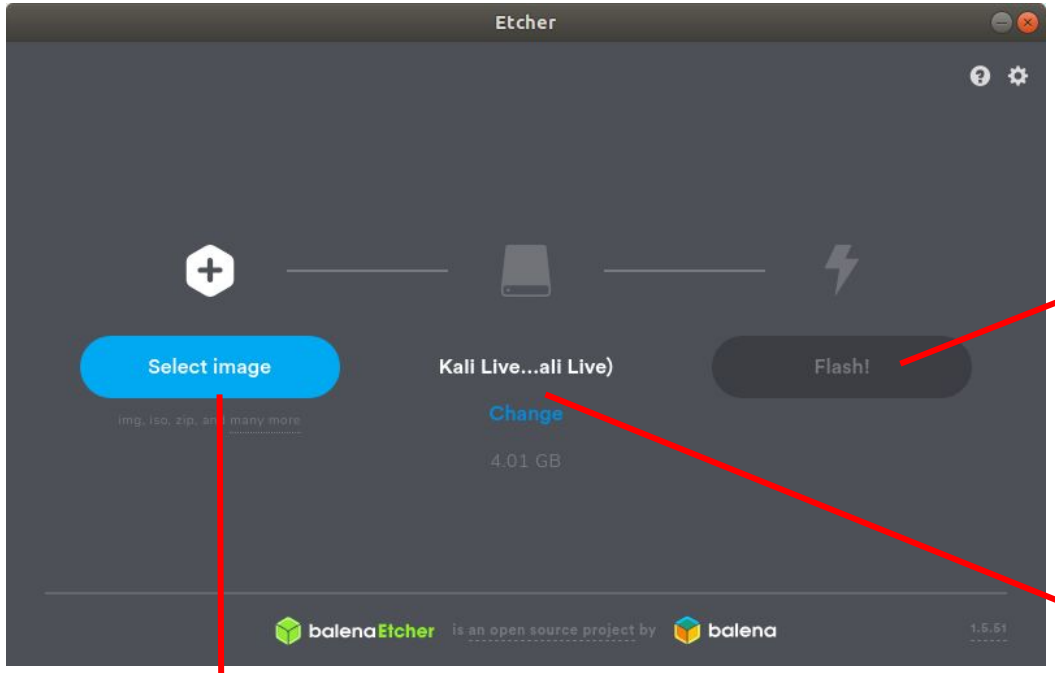
Show in folder

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

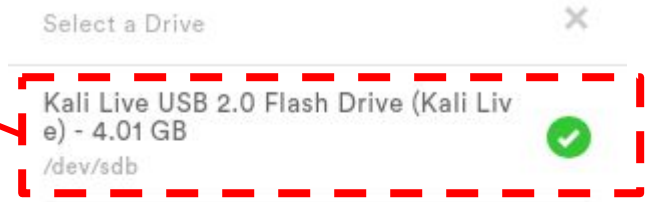
Crear una USB booteable usando como archivo .ISO, la imagen de Kali Linux que se acaba de descargar. Necesitamos una memoria USB de al menos 4 Gb!

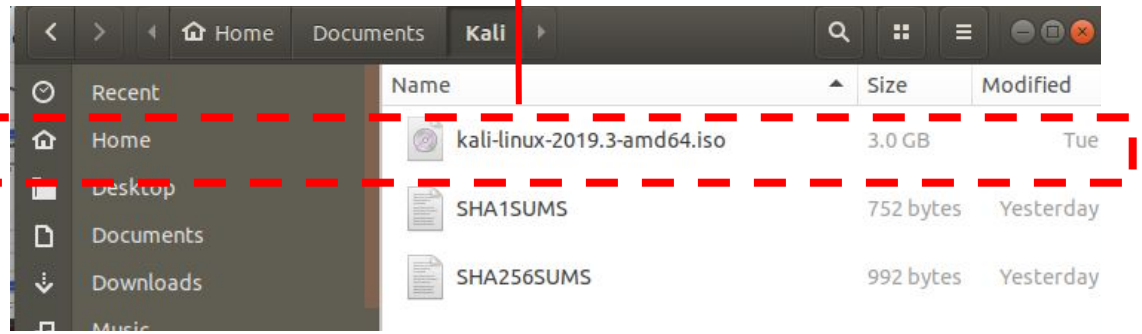


Seguir los pasos que se indican en el siguiente recurso
Desde un equipo Linux: : https://github.com/balena-io/etcher
Desde un equipo Windows: https://tutorials.ubuntu.com/tutorial/tutorial-create-a-usb-stick-on-windows#0

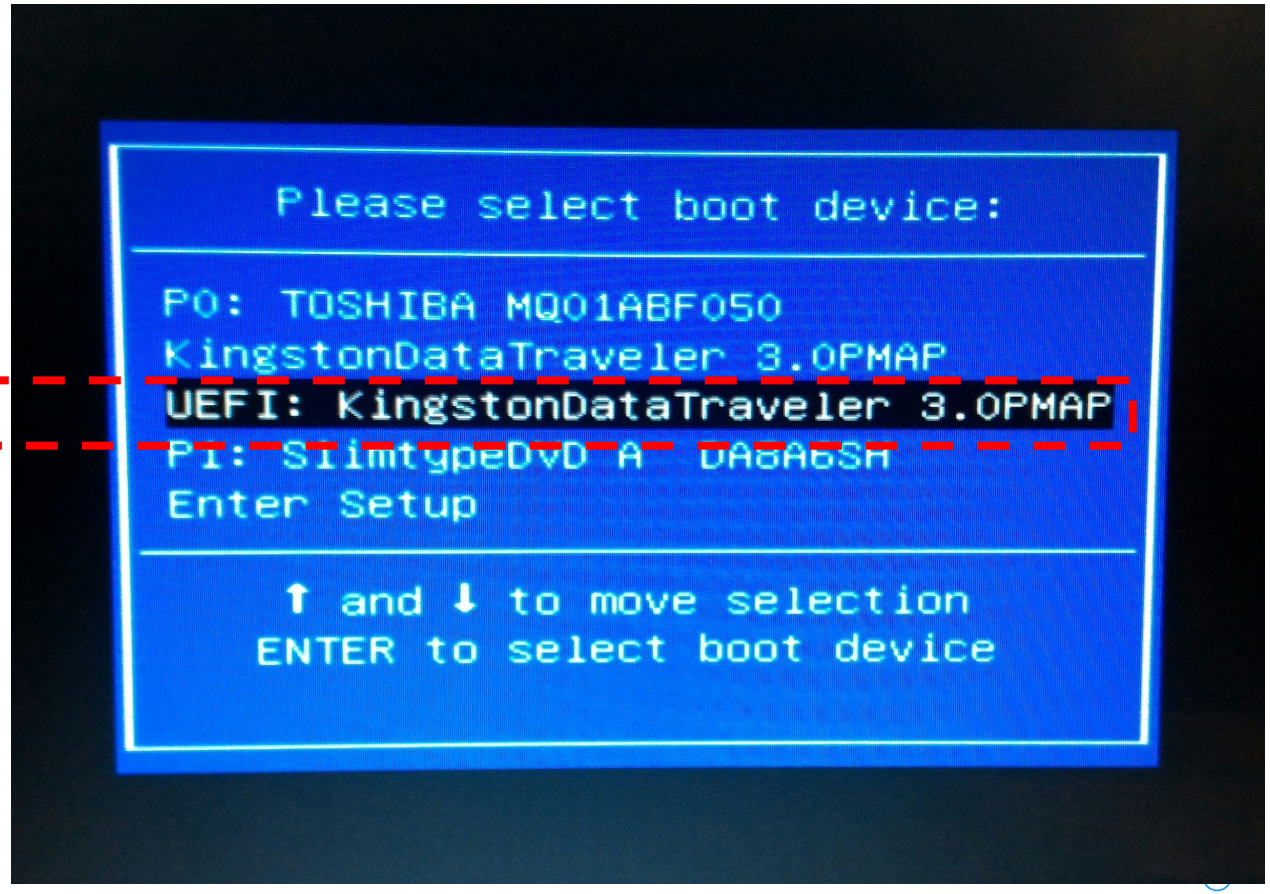


Este botón nos permite iniciar la creación de la memoria USB Bootable!

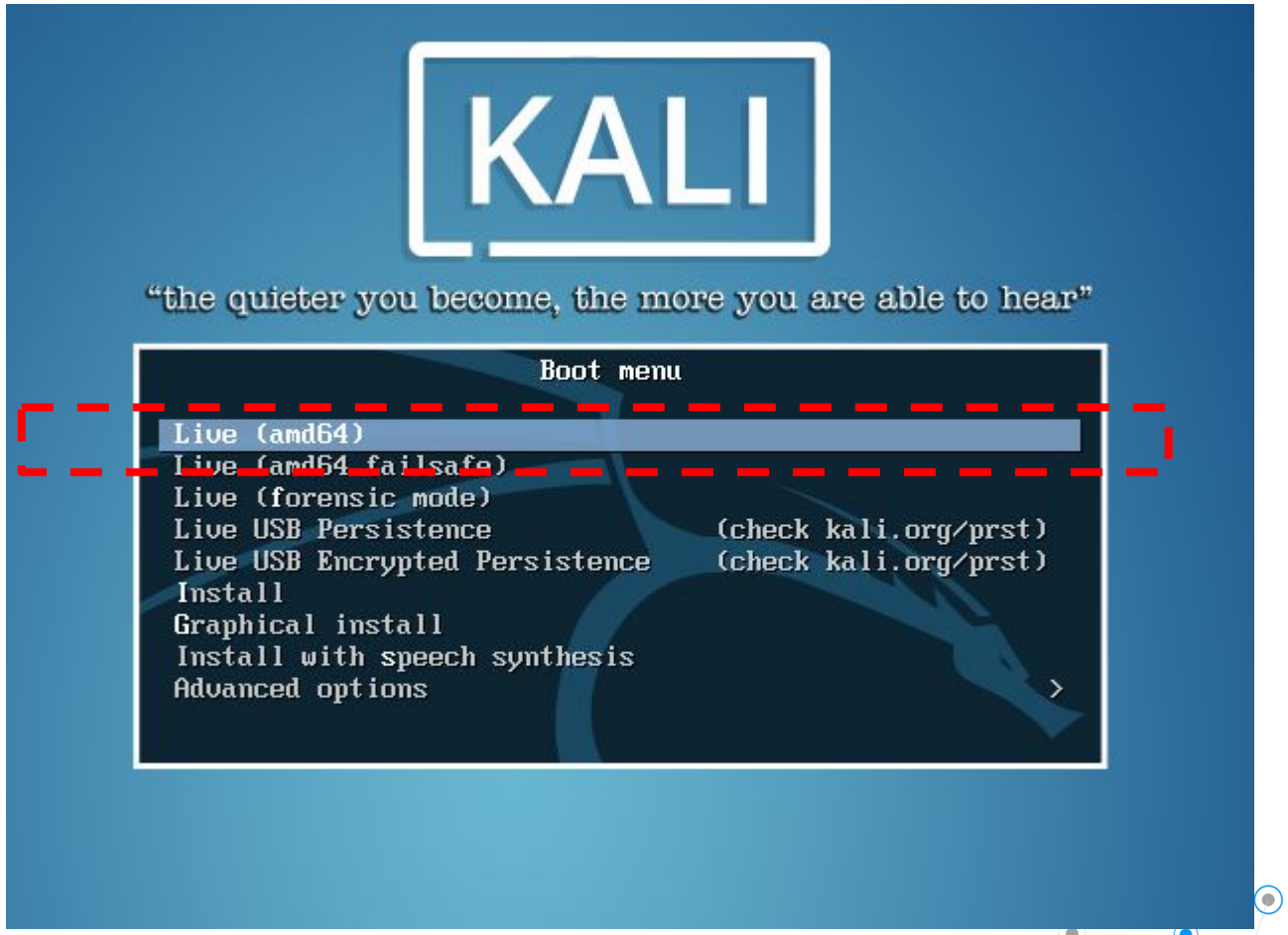




Reiniciar su computador (la memoria con Kali Linux debe estar puesta) y cuando el PC esté encendiendo presionar la tecla **F12** (dependiendo del modelo de su computador puede ser otra otra, sino funciona con F12 intentar con F2, F8, F10) para entrar la “Selección del dispositivo de arranque” y seleccionar la memoria USB en la que está instalado Kali Linux.



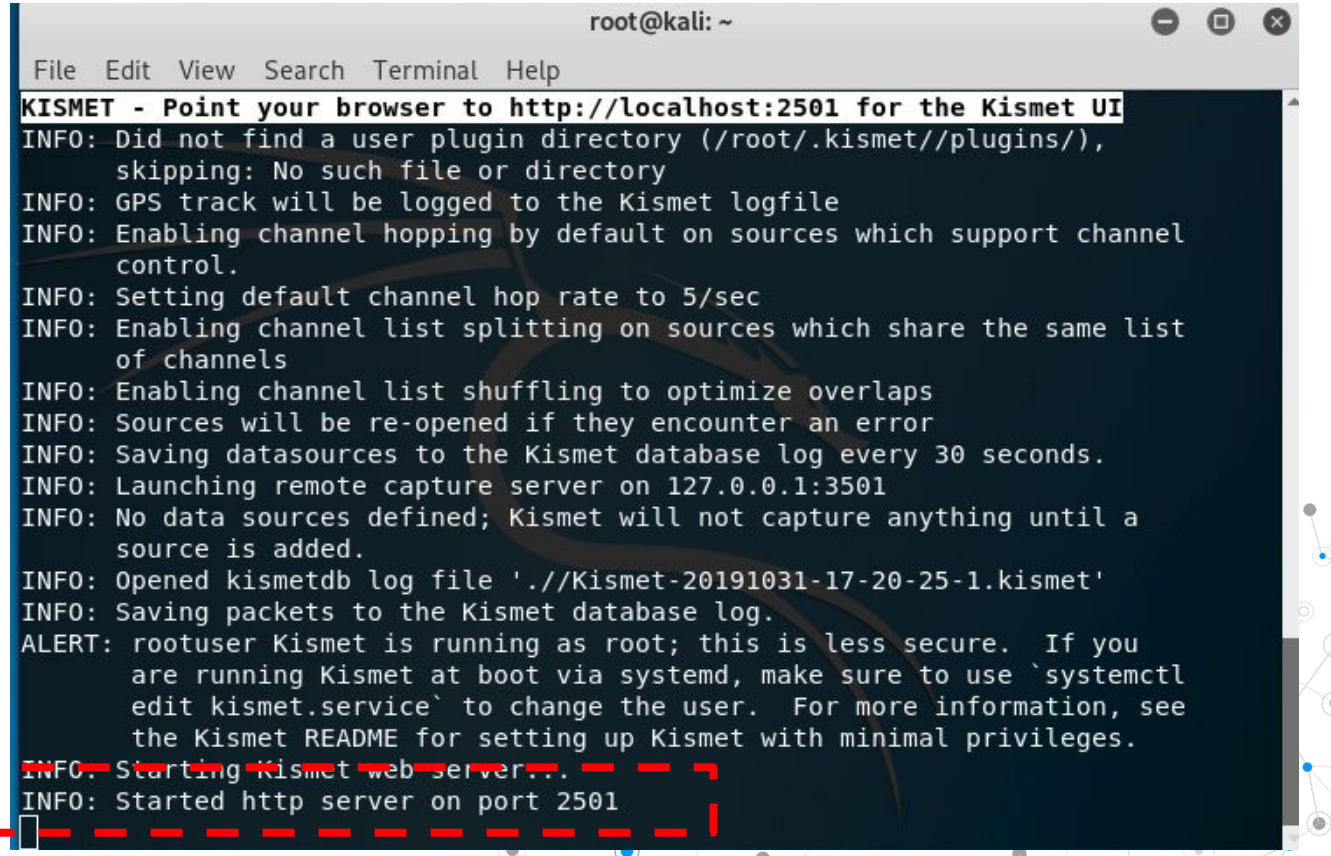
Iniciar Kali Linux en modo **LIVE CD** -> ¡Esto es como si tuvieramos Kali Linux instalado en el computador, pero tan pronto reiniciemos volveremos a tener nuestra instalación anterior y perderemos cualquier archivo guardado en Kali!



Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Desarrollar la siguiente labor de reconocimiento del entorno inalámbrico:

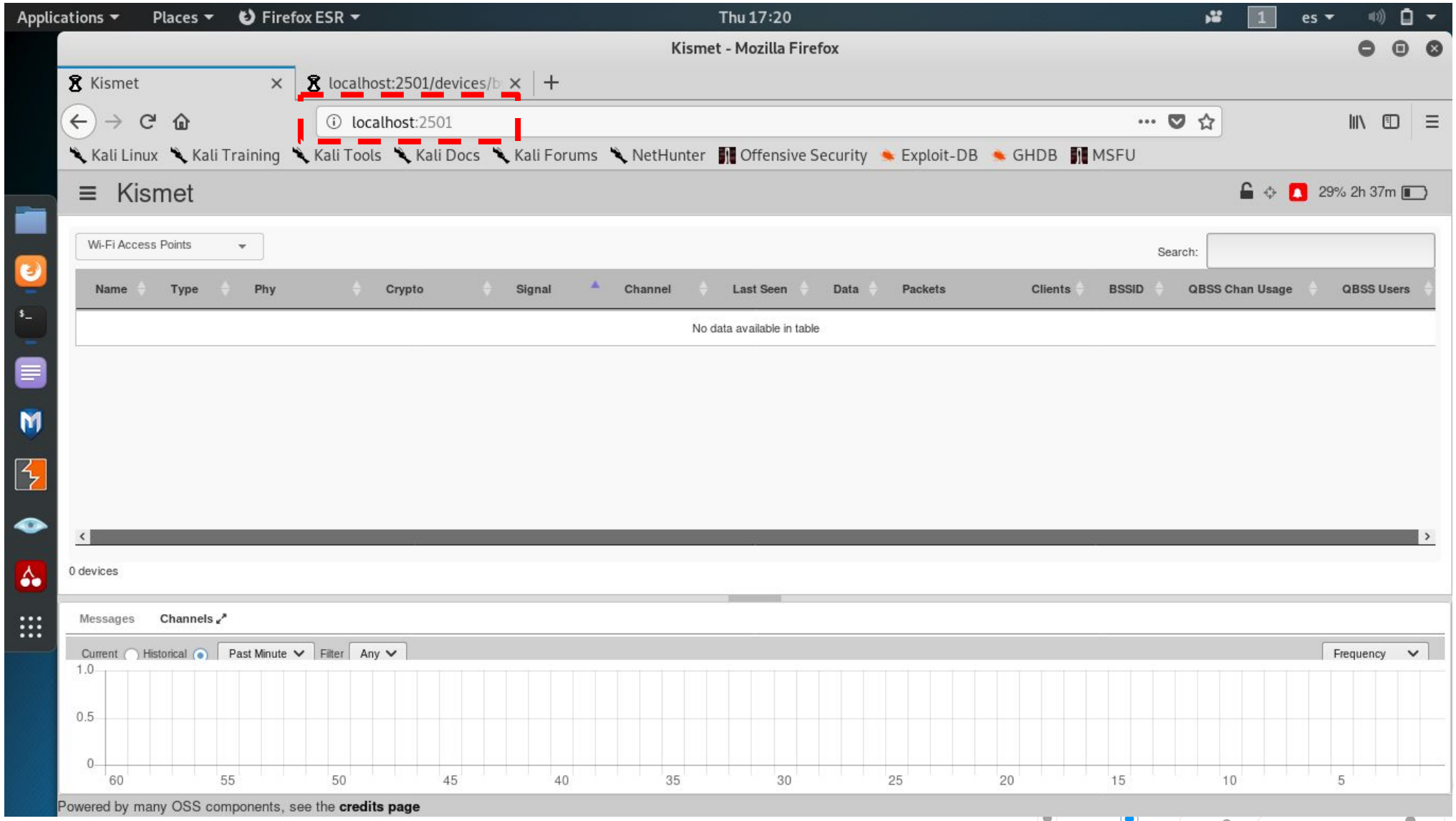
1. Iniciar Kismet desde la consola
2. Acceder a la URL indicada por kismet
3. Monitorear las redes inalámbricas del entorno
4. Responder las preguntas que aparecen al finalizar esta sección



Referencia:

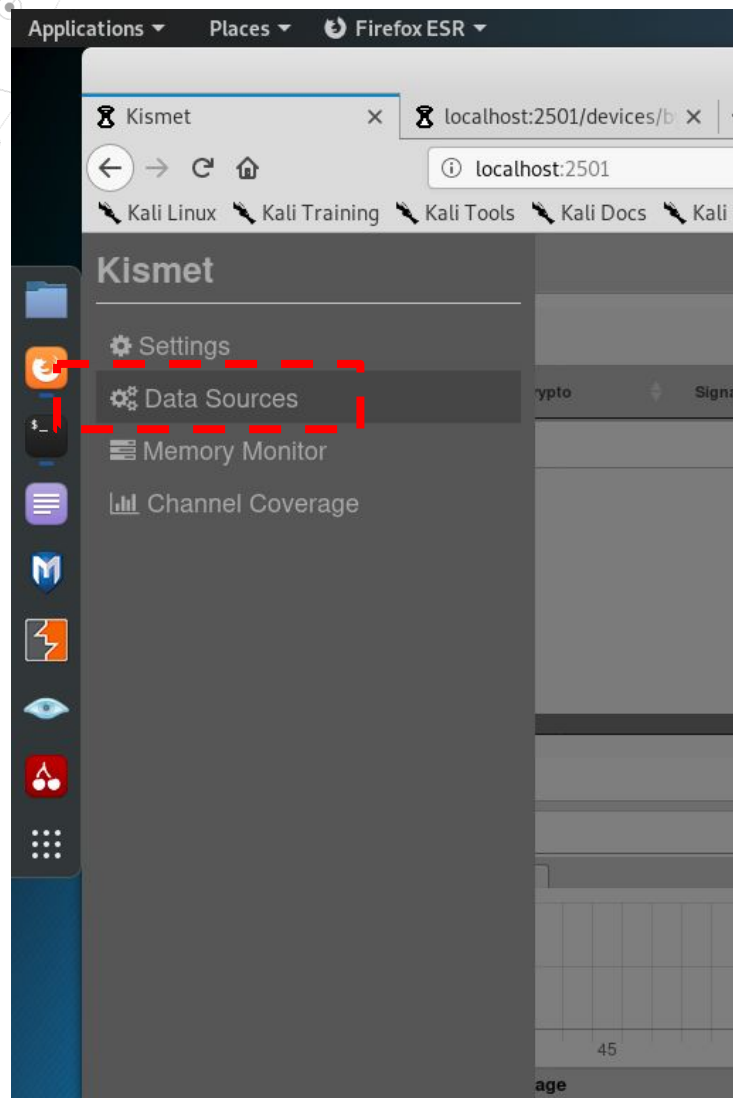
https://tools.kali.org/wireless-attacks/kismet
https://www.kismetwireless.net/#kismet

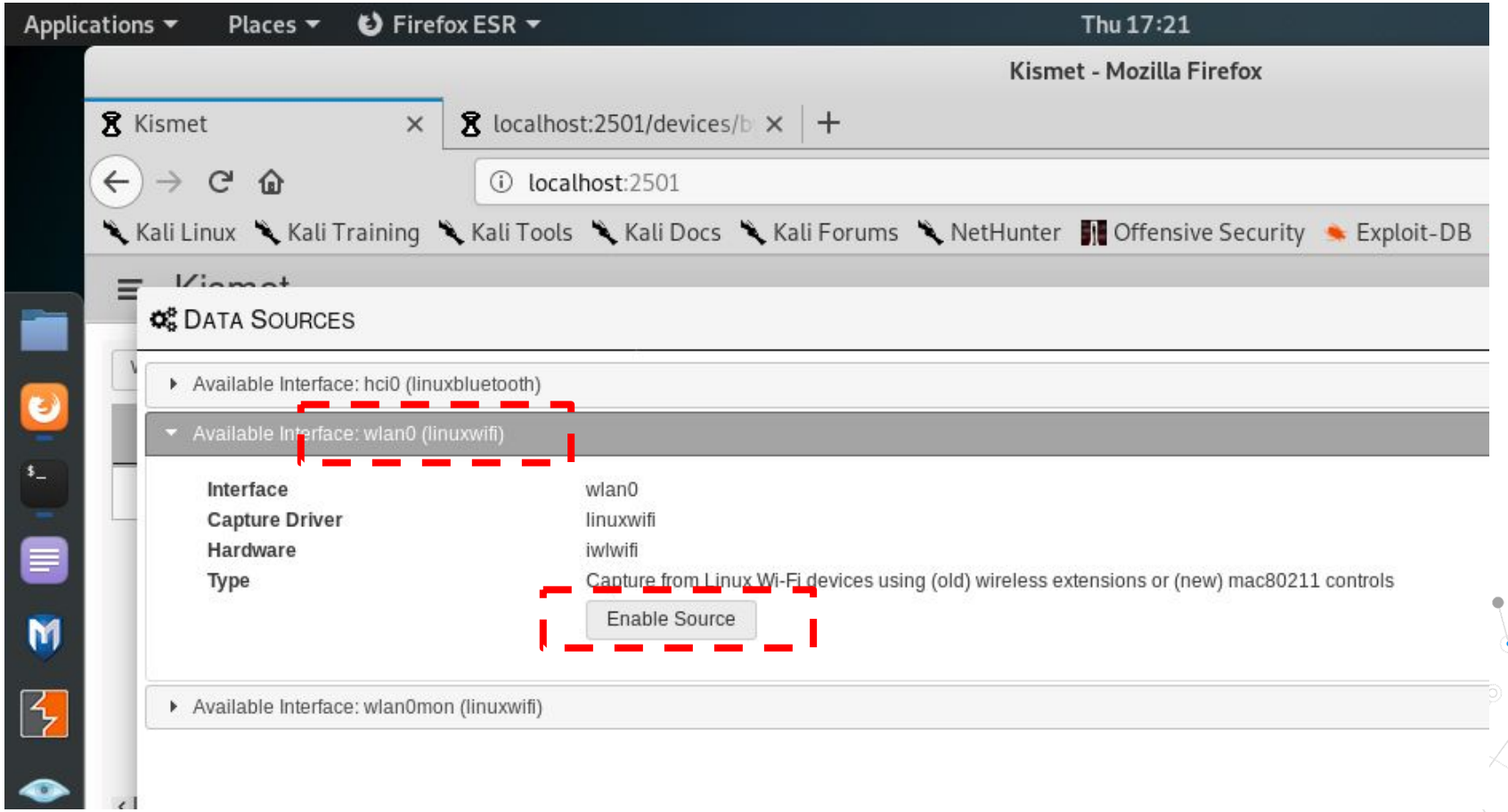
Acceso web a la interfaz de kismet



Habilitación de la fuente de datos para Kismet

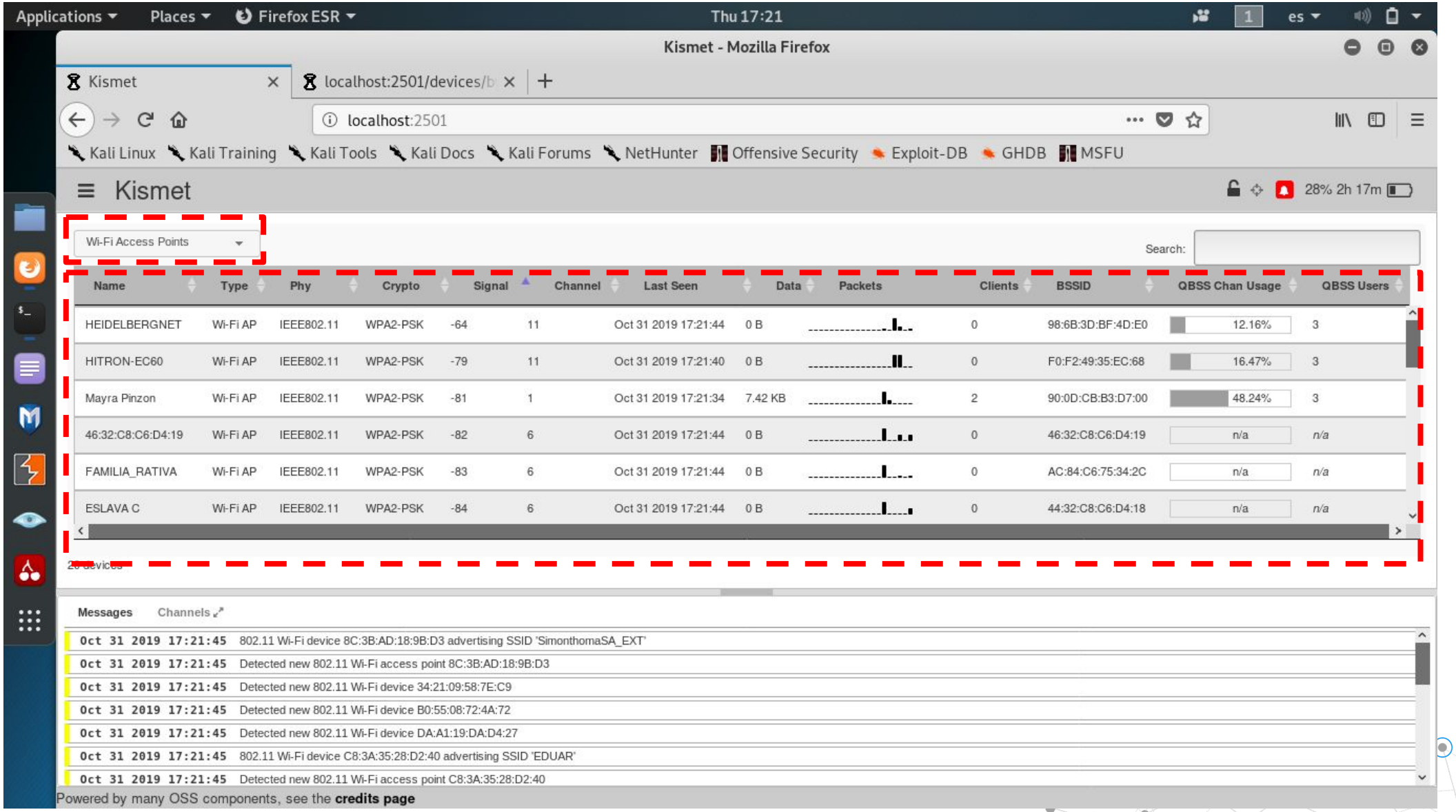
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación





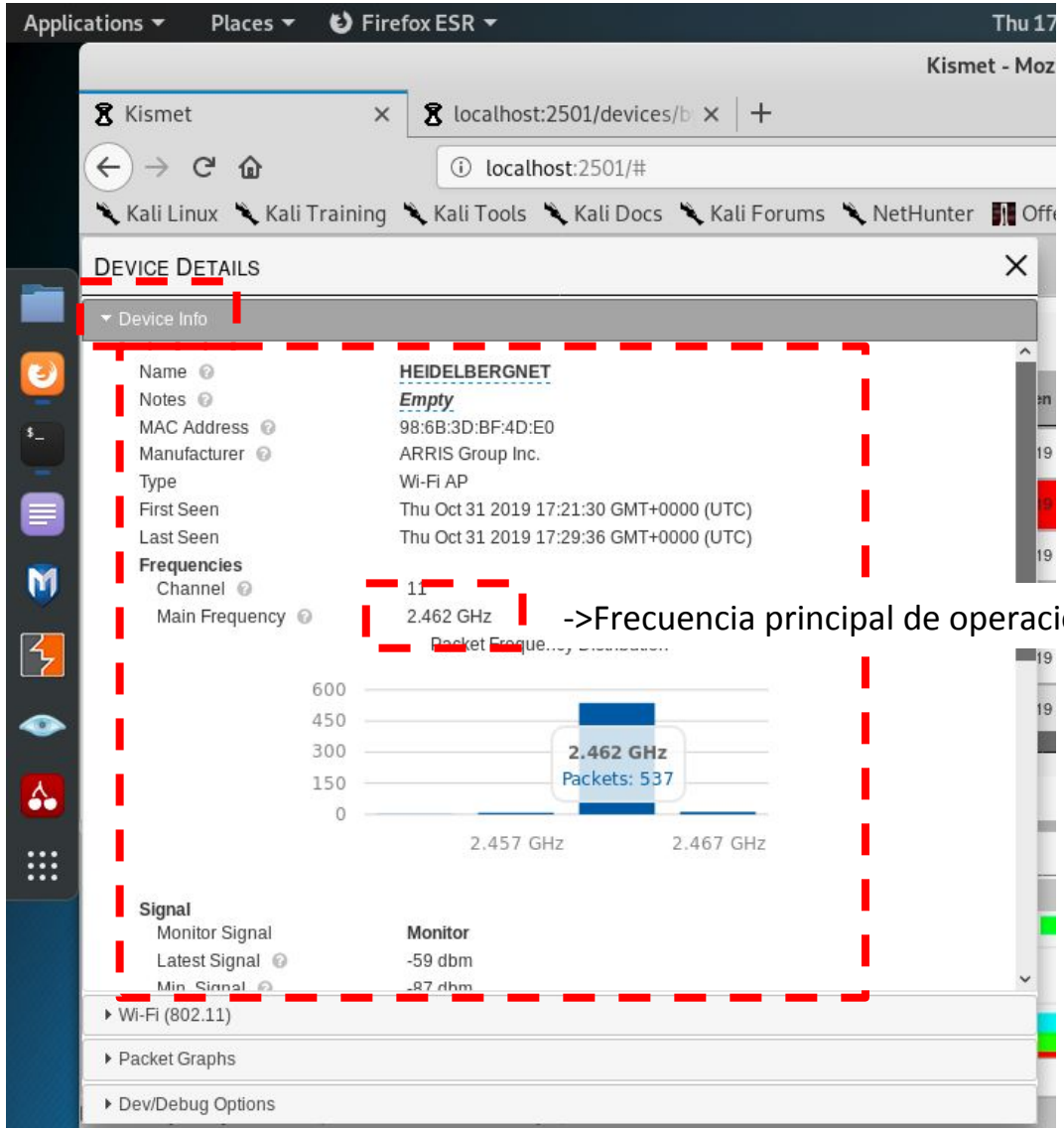
Redes inalámbricas detectadas por kismet

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

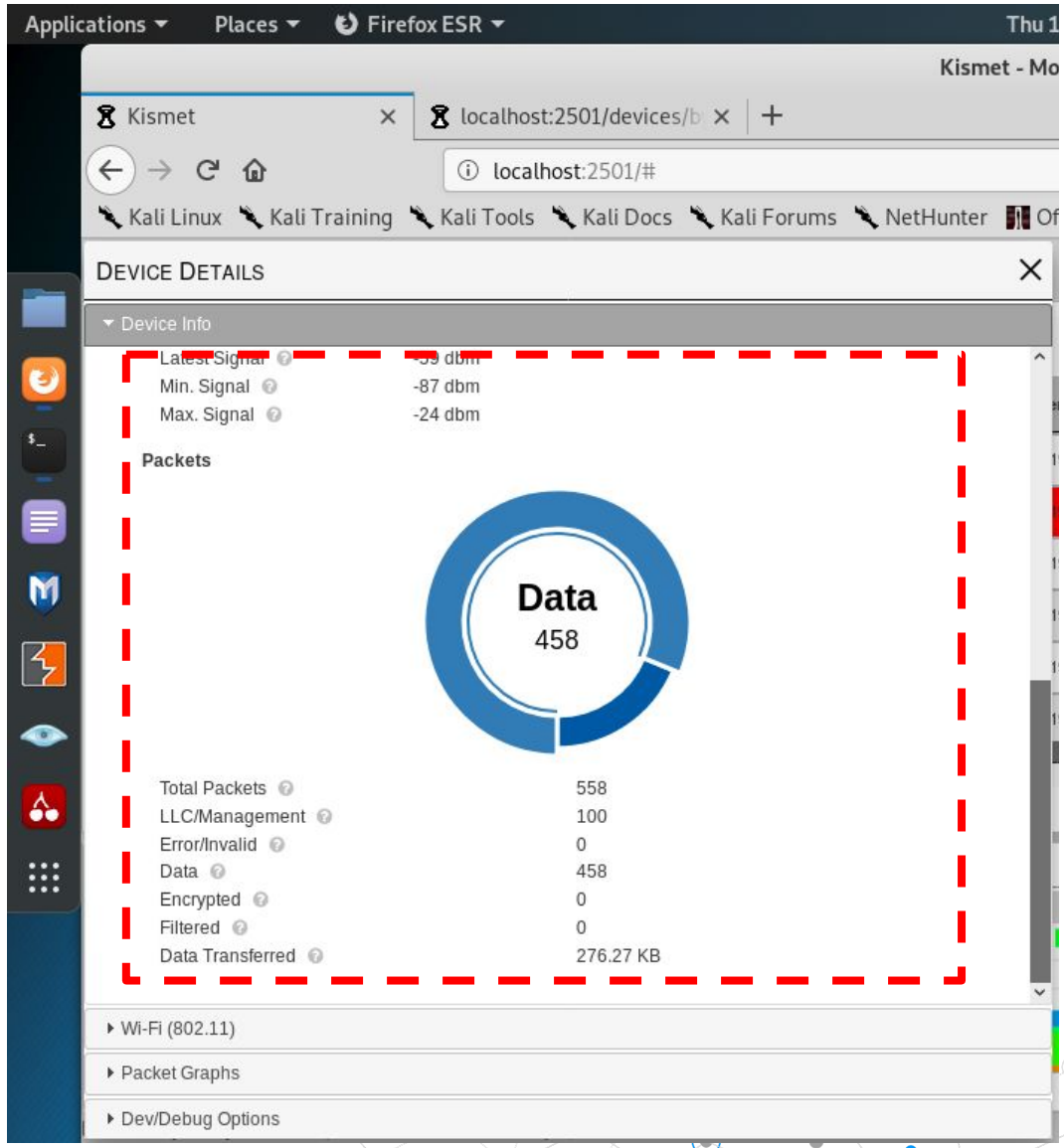


Acceso a la sección “Device Info” de una de las redes detectadas (Heidelbergnet)

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

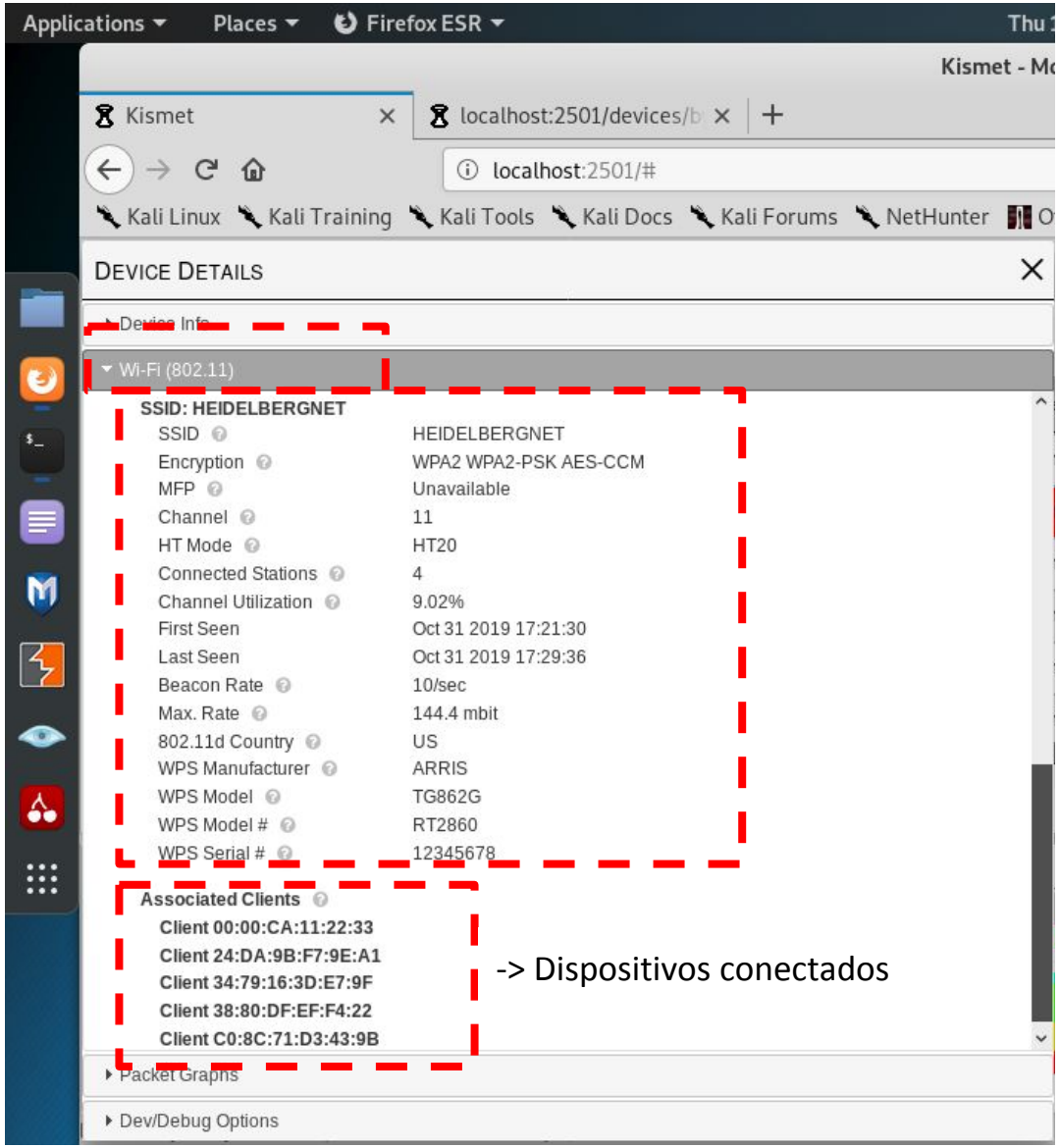


->Frecuencia principal de operación

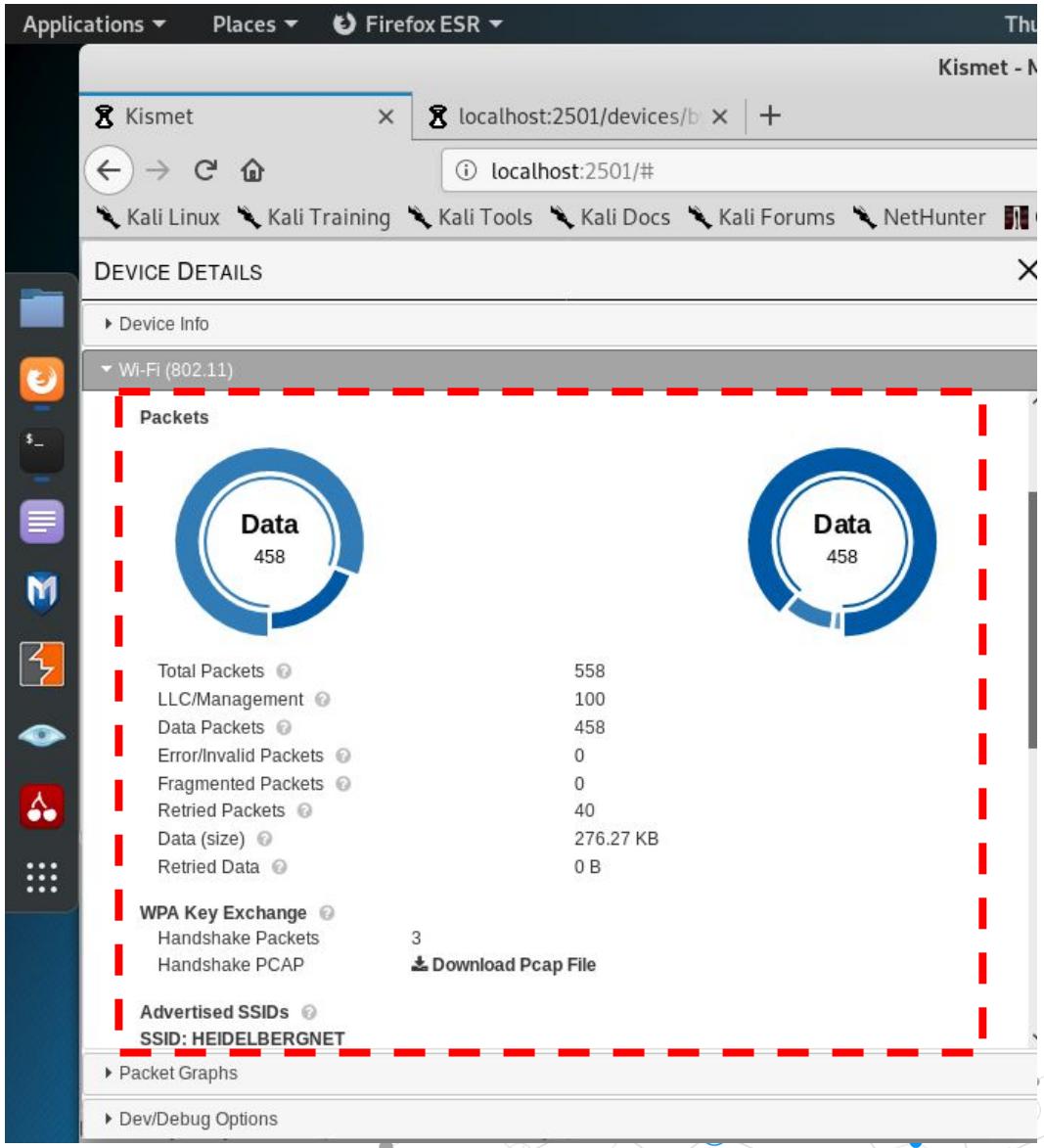


Acceso a la sección “Wi-Fi” de una de las redes detectadas (Heidelbergnet)

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

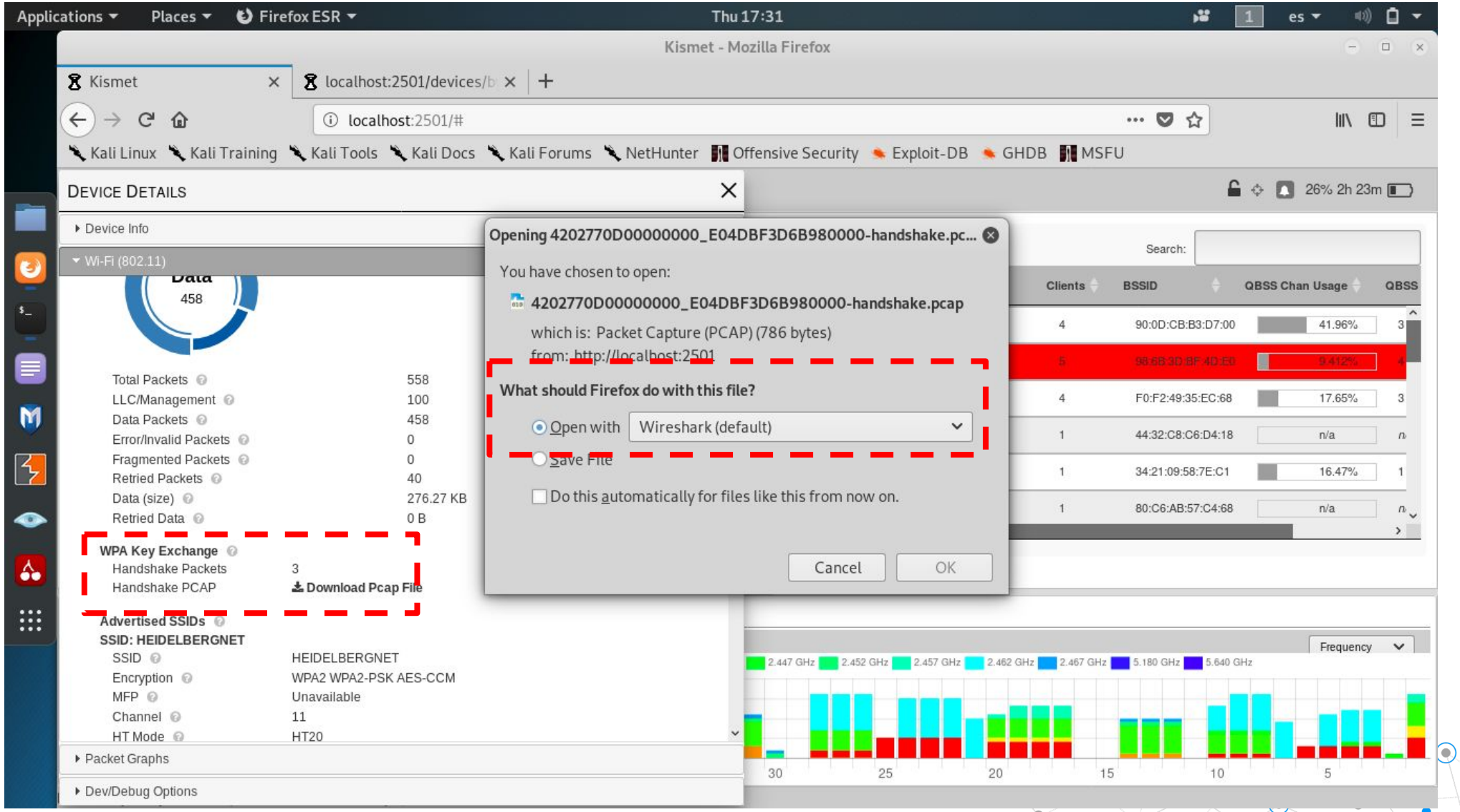


-> Dispositivos conectados



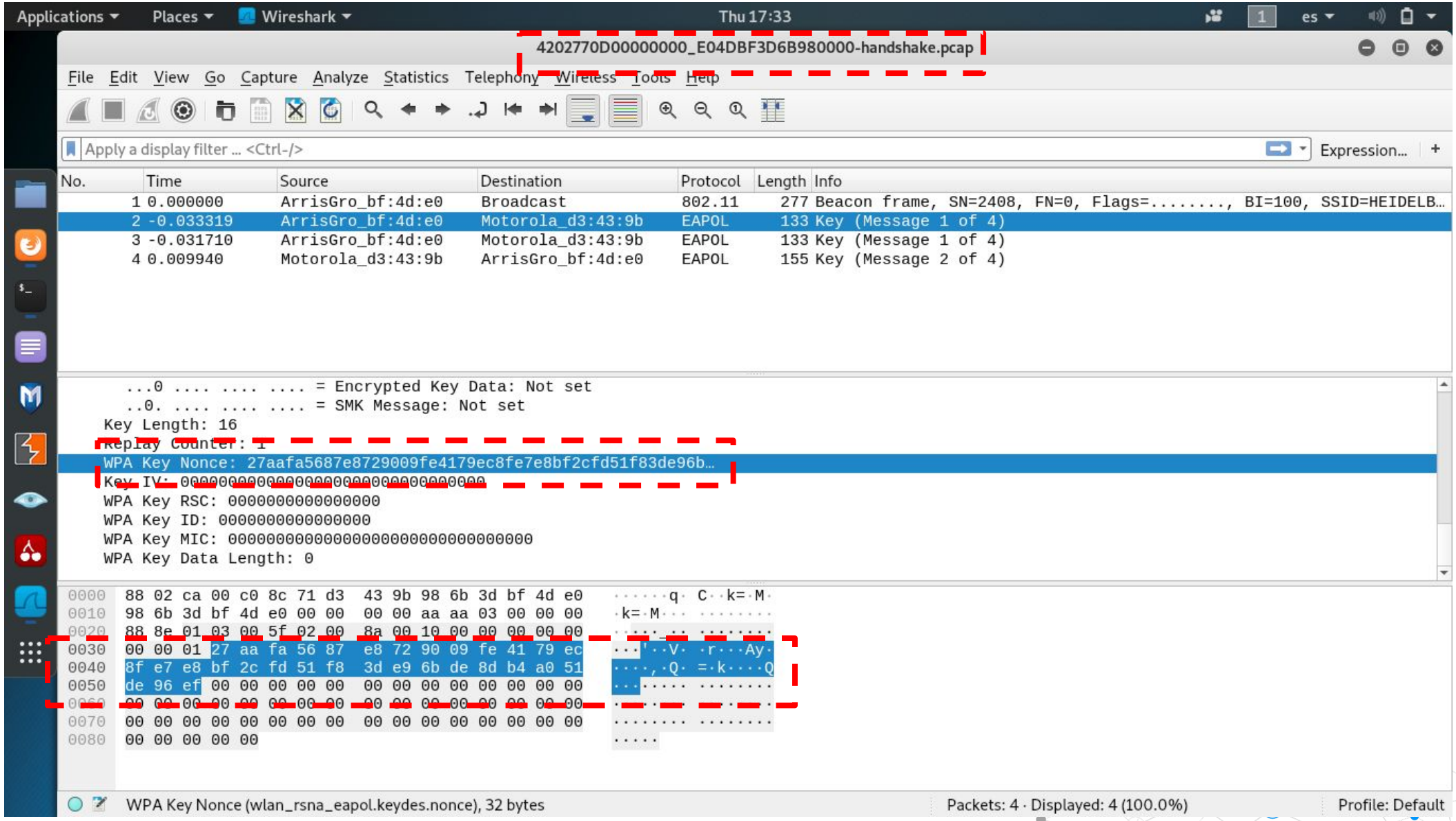
Acceso a los paquetes capturados del handshake en formato PCAP para abrirlos con Wireshark

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



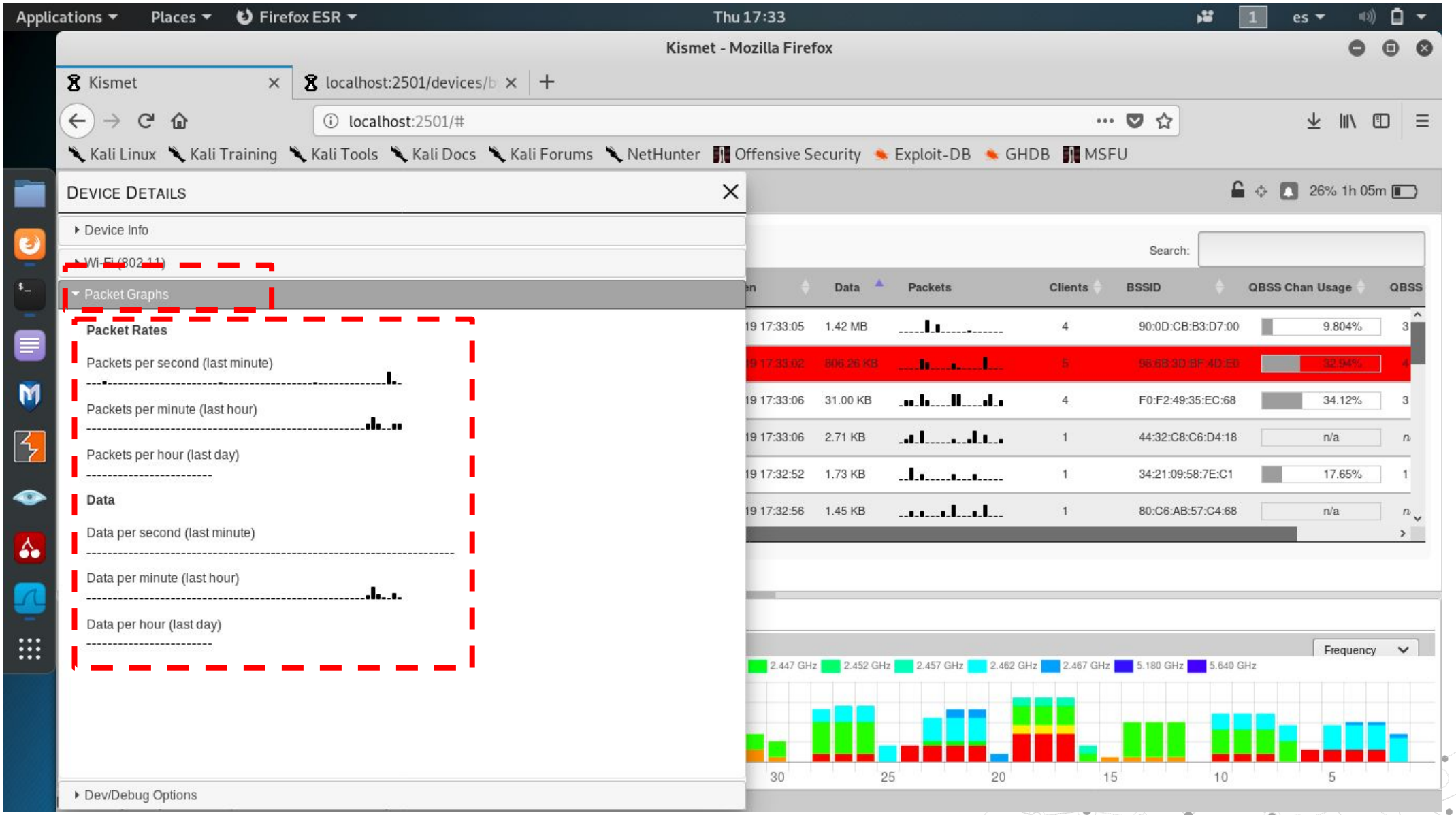
Acceso a los paquetes capturados del handshake en formato PCAP para abrirlos con Wireshark

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



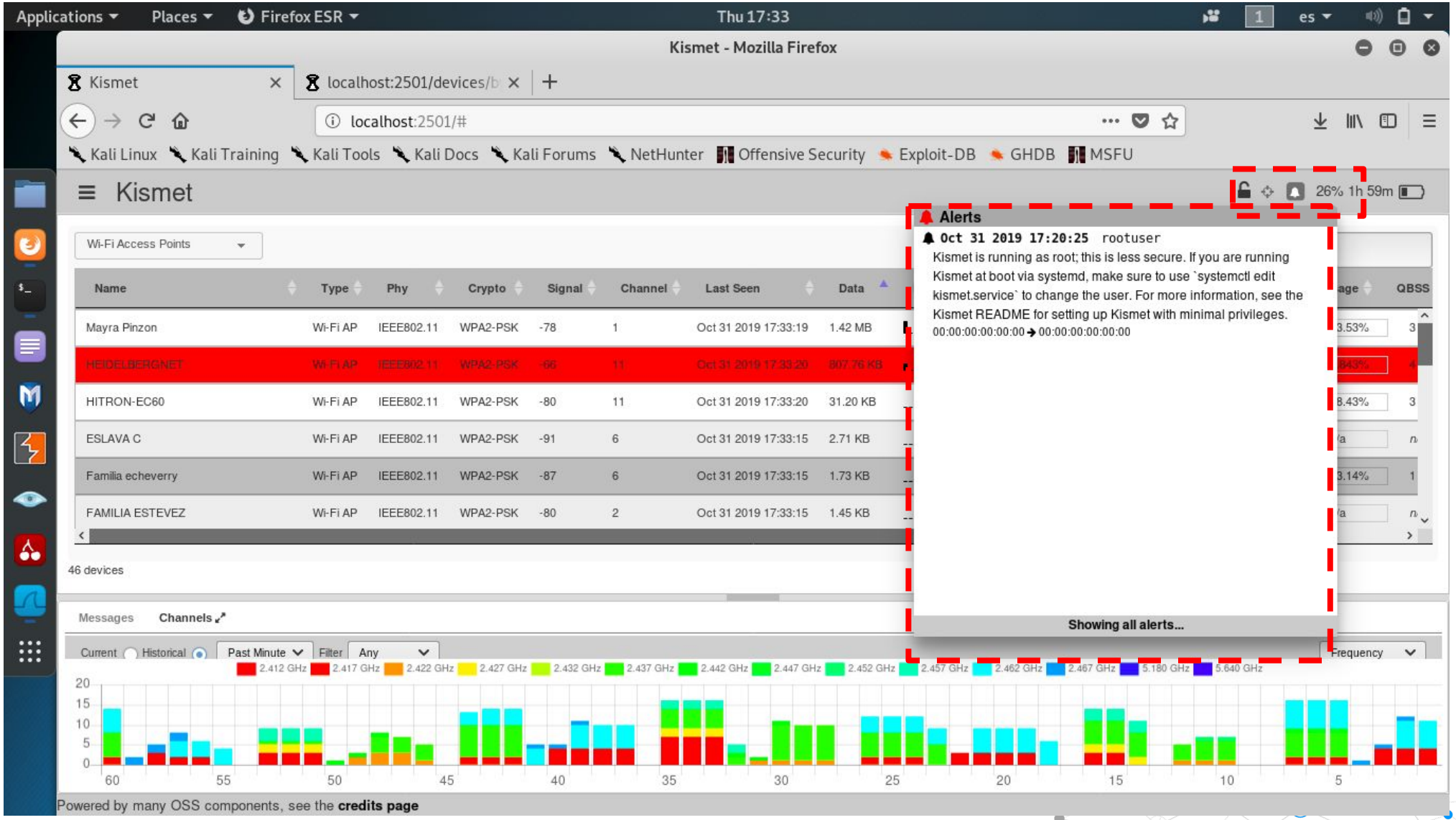
Acceso a la sección “Packet Graphs” de una de las redes detectadas (Heidelbergnet)

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



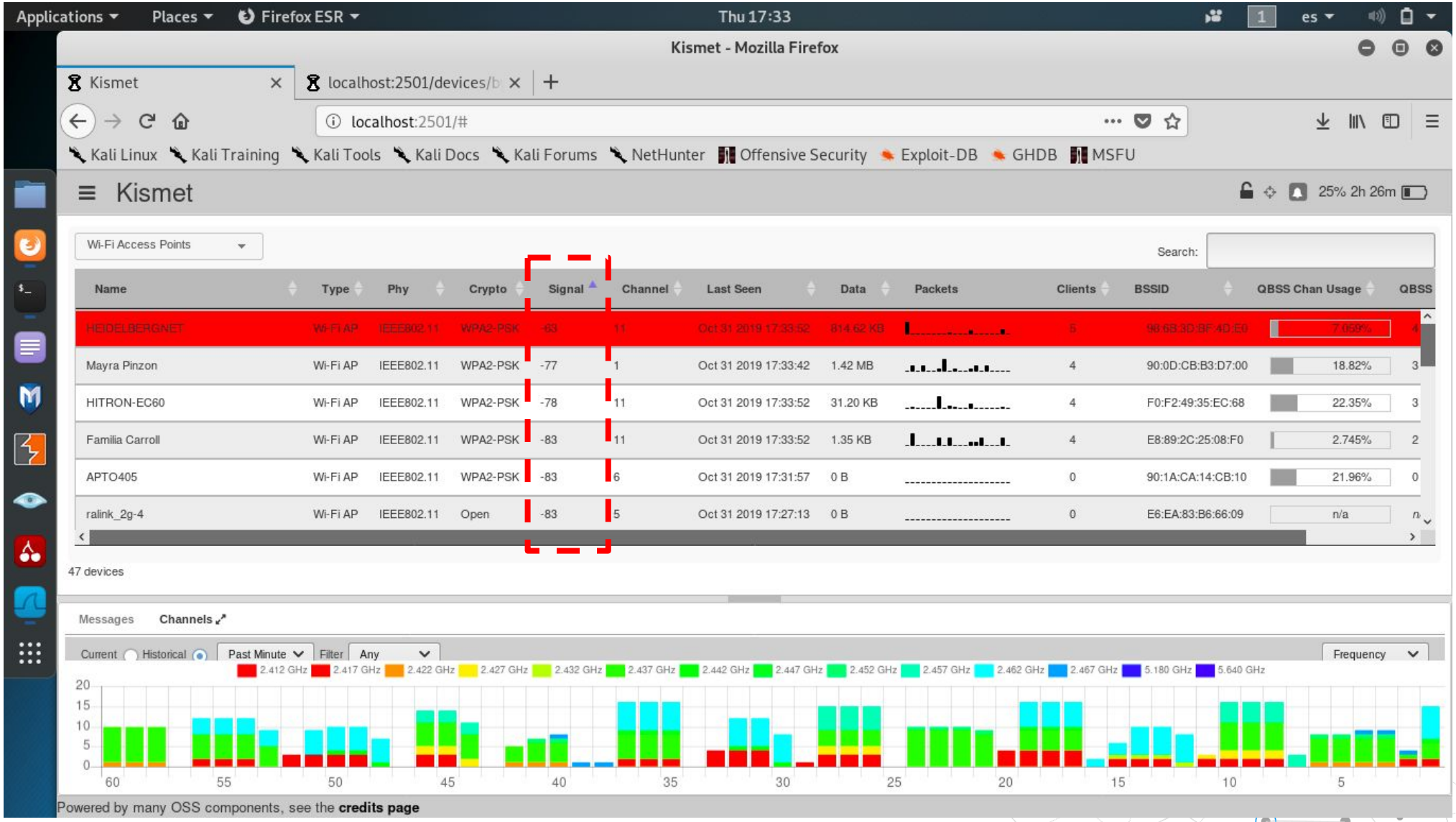
Alertas detectadas por Kismet para todas las redes inalámbricas detectadas

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



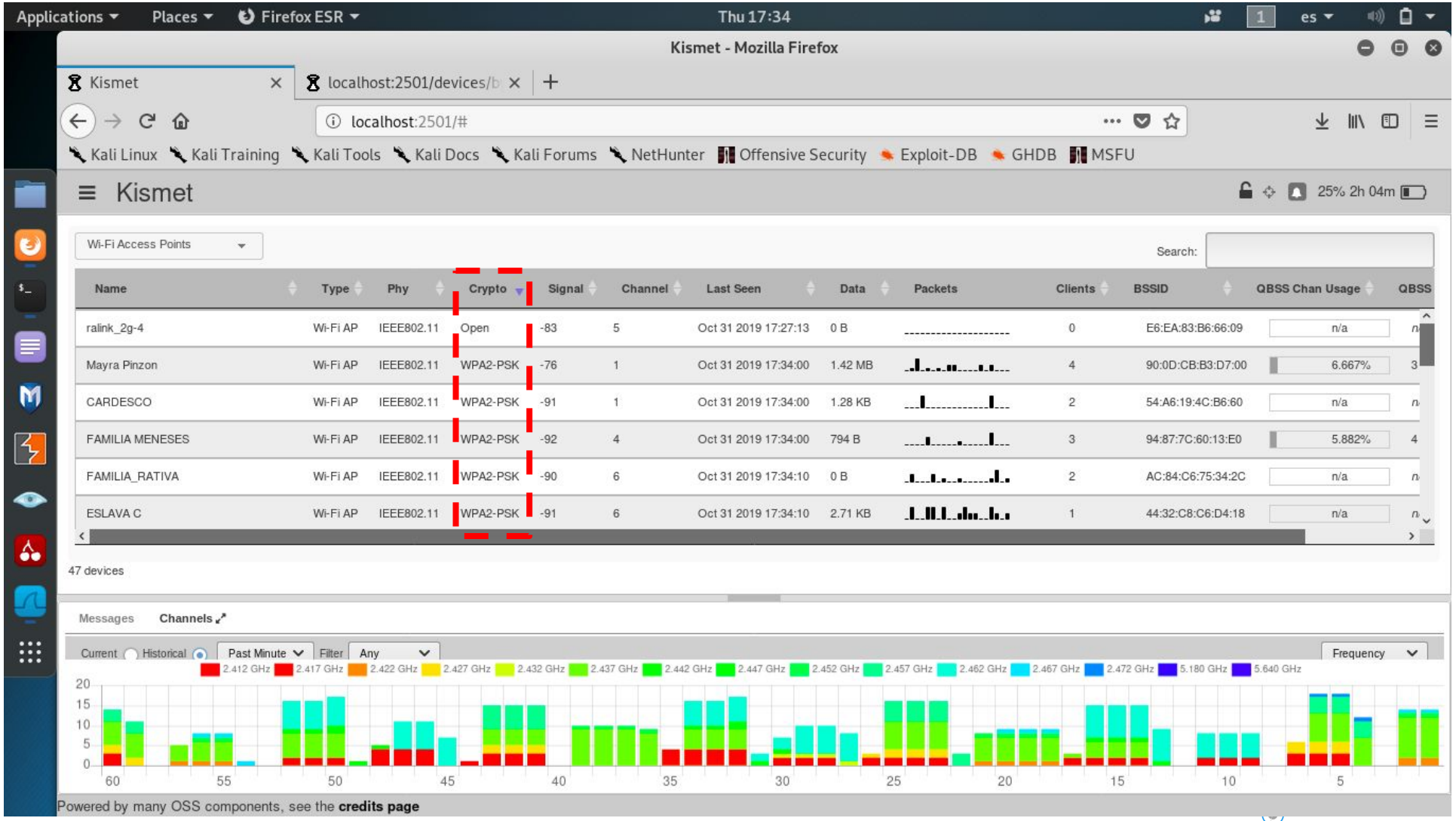
Ordenación de redes por nivel de señal (Mayor a menor)

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



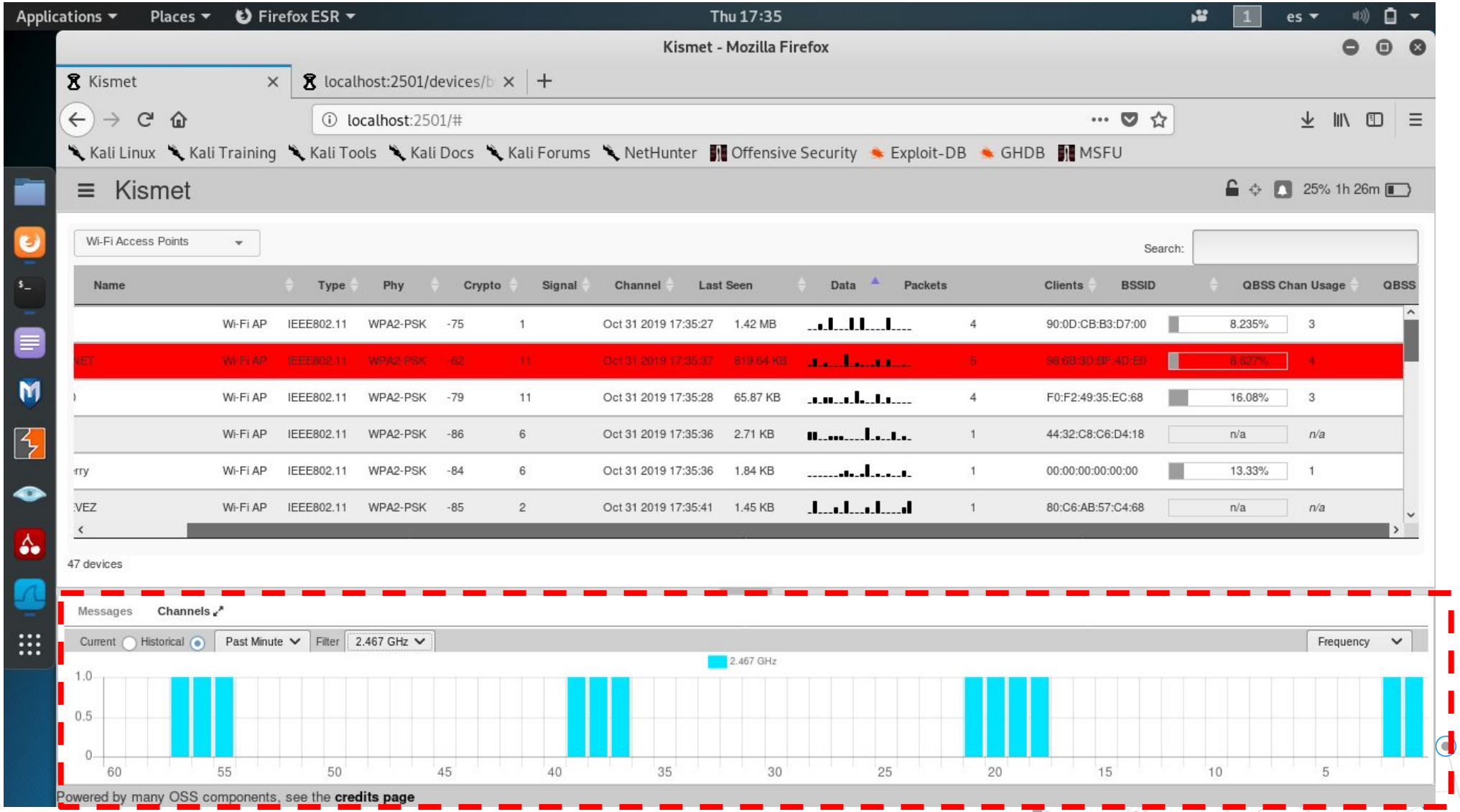
Ordenación de redes por tipo de cifrado (Redes abiertas al principio)

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



Dispositivos transmitiendo en la frecuencia 2.46 Ghz

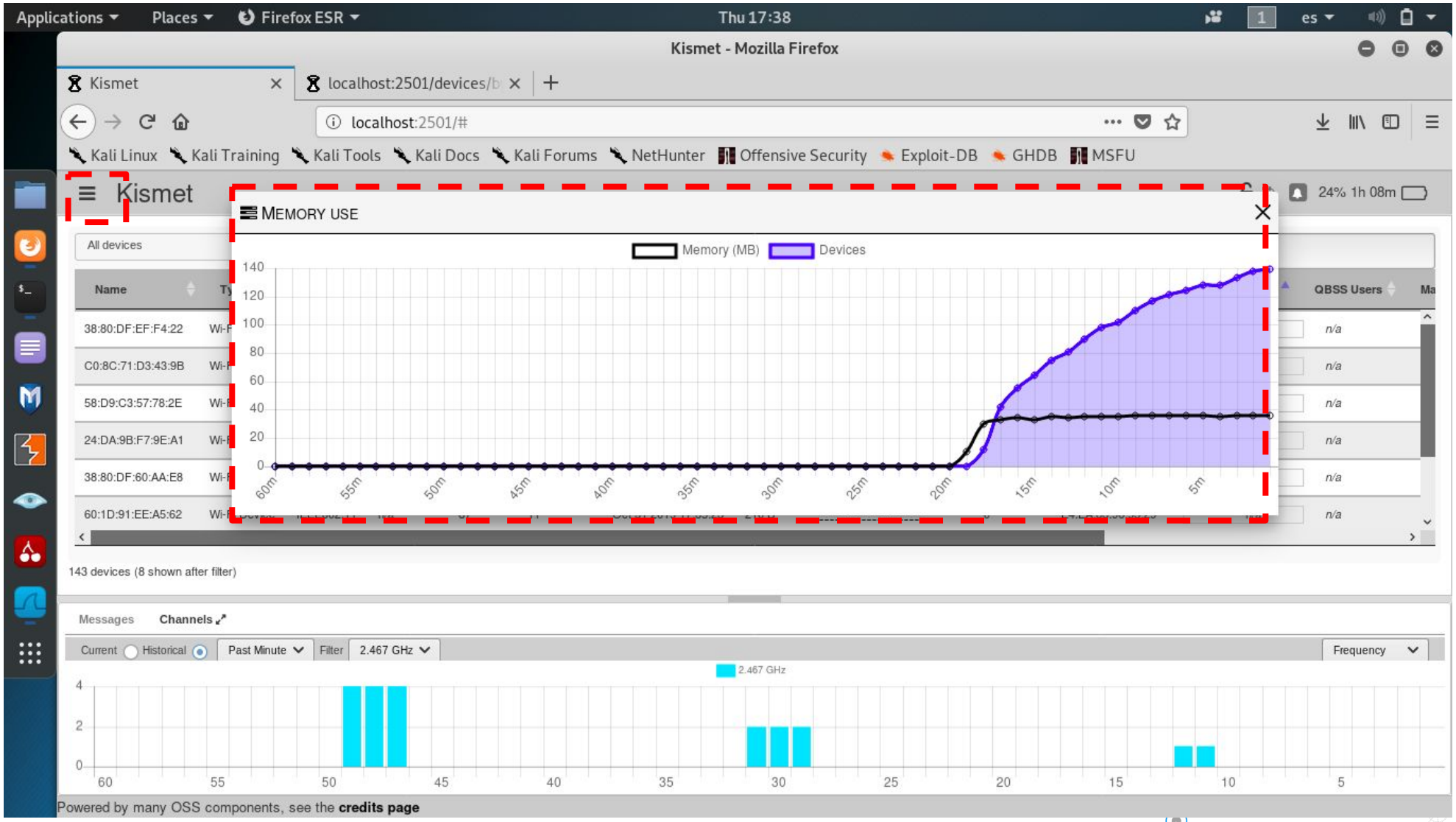
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación



Número de dispositivos detectados por kismet y consumo de RAM por parte de Kismet

Universidad del Rosario

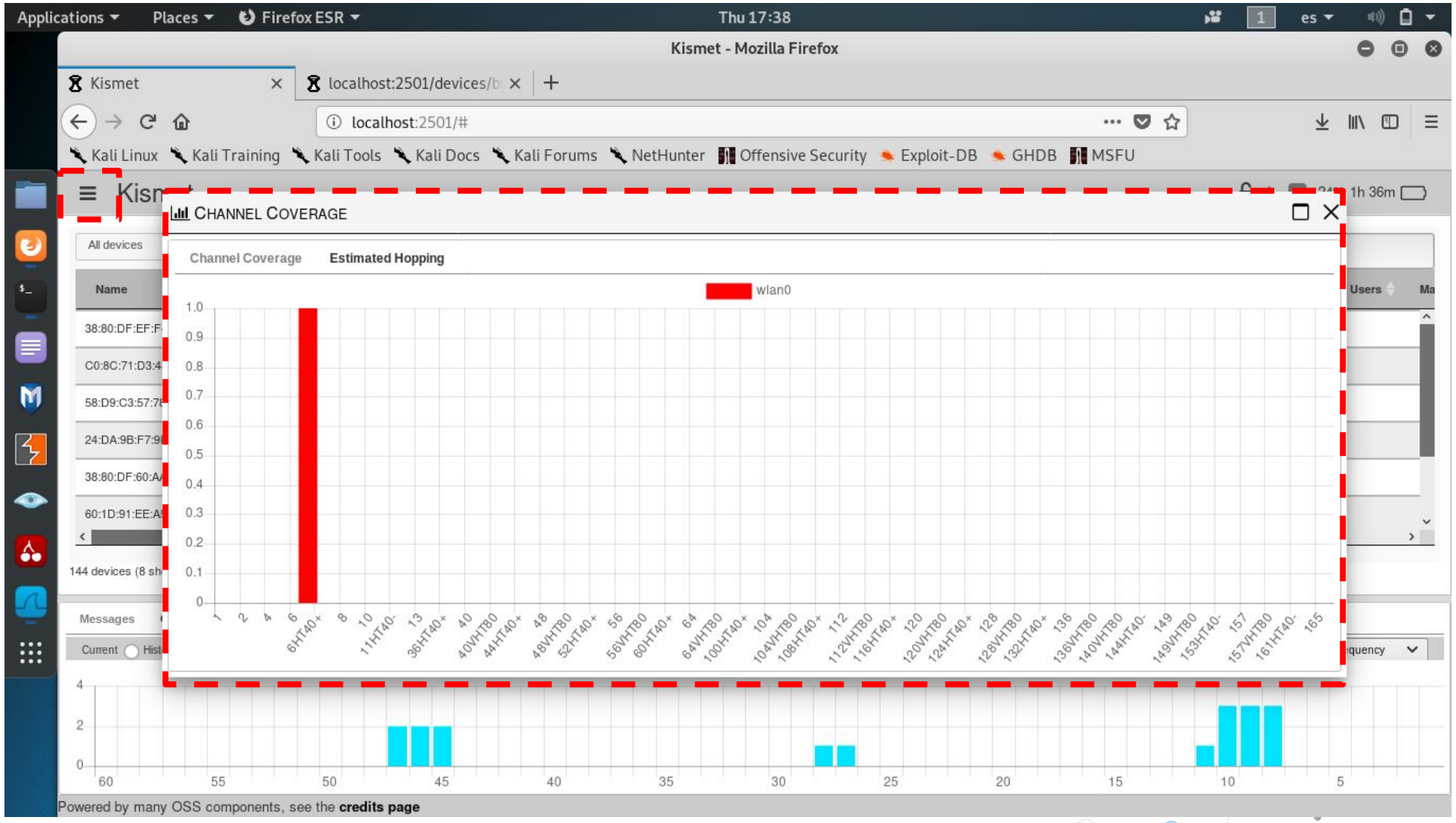
MACC
Matemáticas Aplicadas y Ciencias de la Computación



Salto de frecuencia realizado por Kismet para poder detectar dispositivos en diferentes frecuencias

Universidad del Rosario

MACC
Matemáticas Aplicadas y Ciencias de la Computación



PREGUNTAS

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

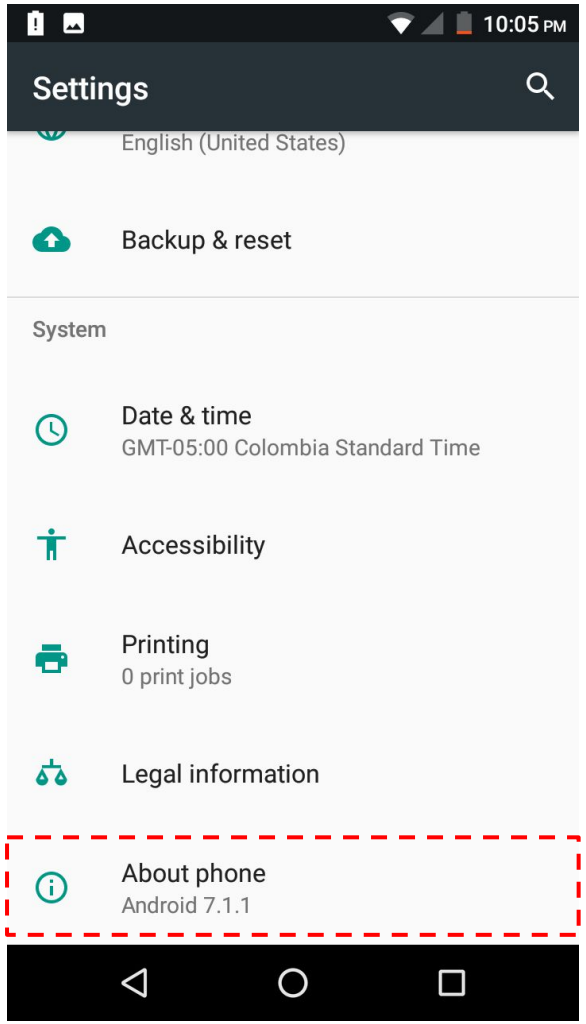
Ejecute Kismet en un laptop que tenga en casa y resuelva las siguientes preguntas mostrando la evidencia (Captura de pantalla):

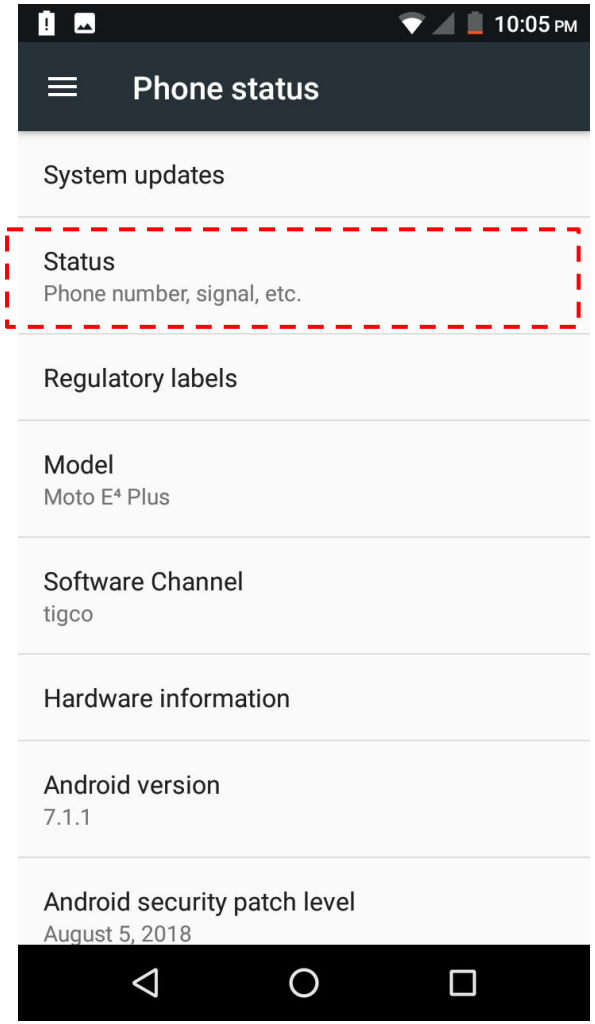
- ¿Cuantas redes en total detecta en las proximidades de su hogar?
- ¿Cuántas y cuáles redes inalámbricas ocultas detecta?
- ¿Cuantos BSSID detecta, de ejemplo de algunos de ellos?
- Ordene las redes inalámbricas detectadas por SIGNAL (Mayor a Menor) y detecte las de mayor señal. ¿Que es un dB?
- Ordene las redes inalámbricas detectadas por CRYPT (Menor a Menor) y detecte las de cifrado más débiles
- ¿Kismet detecta alguna alarma? ¿Cuales? Expliquelas teniendo como base la siguiente documentación: https://www.kismetwireless.net/docs/readme/alerts_and_wids/

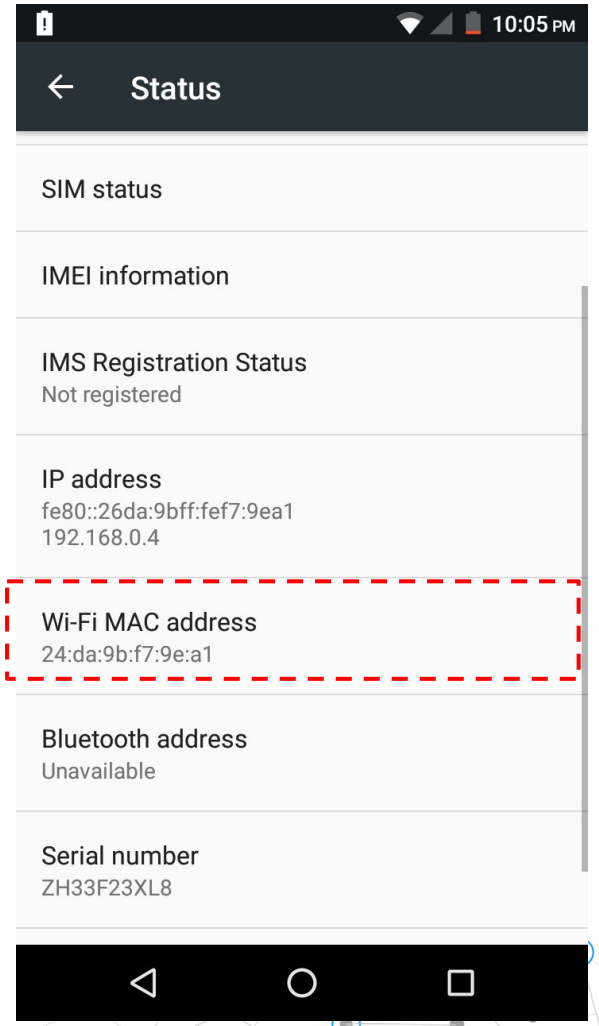
- Si accede a la información de los clientes conectados a la red de su casa (slide anterior), ¿Reconoce todos los dispositivos como de confianza o encuentra alguno sospechoso? (Revise su dirección MAC como se indica en el siguiente slide)
- ¿Cuánto tiempo lleva encendido su Router de hogar? (Esto puede ser un indicio de lo desactualizado que puede estar)
- ¿Cual es la frecuencia principal que su router de hogar utiliza para las comunicaciones con los clientes?
- ¿Cual es el cifrado que utiliza su router de hogar?
- ¿Cual es la relación entre el “Data Packet” y el “Management Packet” para su router de hogar?

Rate = “Data Packet” / “Management Packet”

Consultar la dirección MAC de un equipo Android:







(Opcional) Desplegar un HOTSPOT falso que suplante una red inalámbrica

1. Instalar wifi honey siguiendo la documentación de referencia
2. Configurar wifi honey para suplantar una red inalámbrica y reconocer a los dispositivos que se intenten conectar a ella.
   Explicar todos los resultados encontrados.

Referencia:
https://tools.kali.org/wireless-attacks/wifi-honey
https://digi.ninja/projects/wifi_honey.php

wifi-honey – Wi-Fi honeypot

```
root@kali:~# wifi-honey -h
Usage: /usr/bin/wifi-honey <essid> <channel> <interface>

Default channel is 1
Default interface is wlan0

Robin Wood <robin@digininja.org>
See Security Tube Wifi Mega Primer episode 26 for more information
```

wifi-honey Usage Example

Broadcast the given ESSID ***(FreeWiFi)*** on channel 6 ***(6)*** using the wireless interface ***(wlan0)***:

```
root@kali:~# wifi-honey FreeWiFi 6 wlan0
```

Universidad del Rosario | MACC | HINNT

¡Gracias!