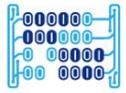




Universidad del  
Rosario



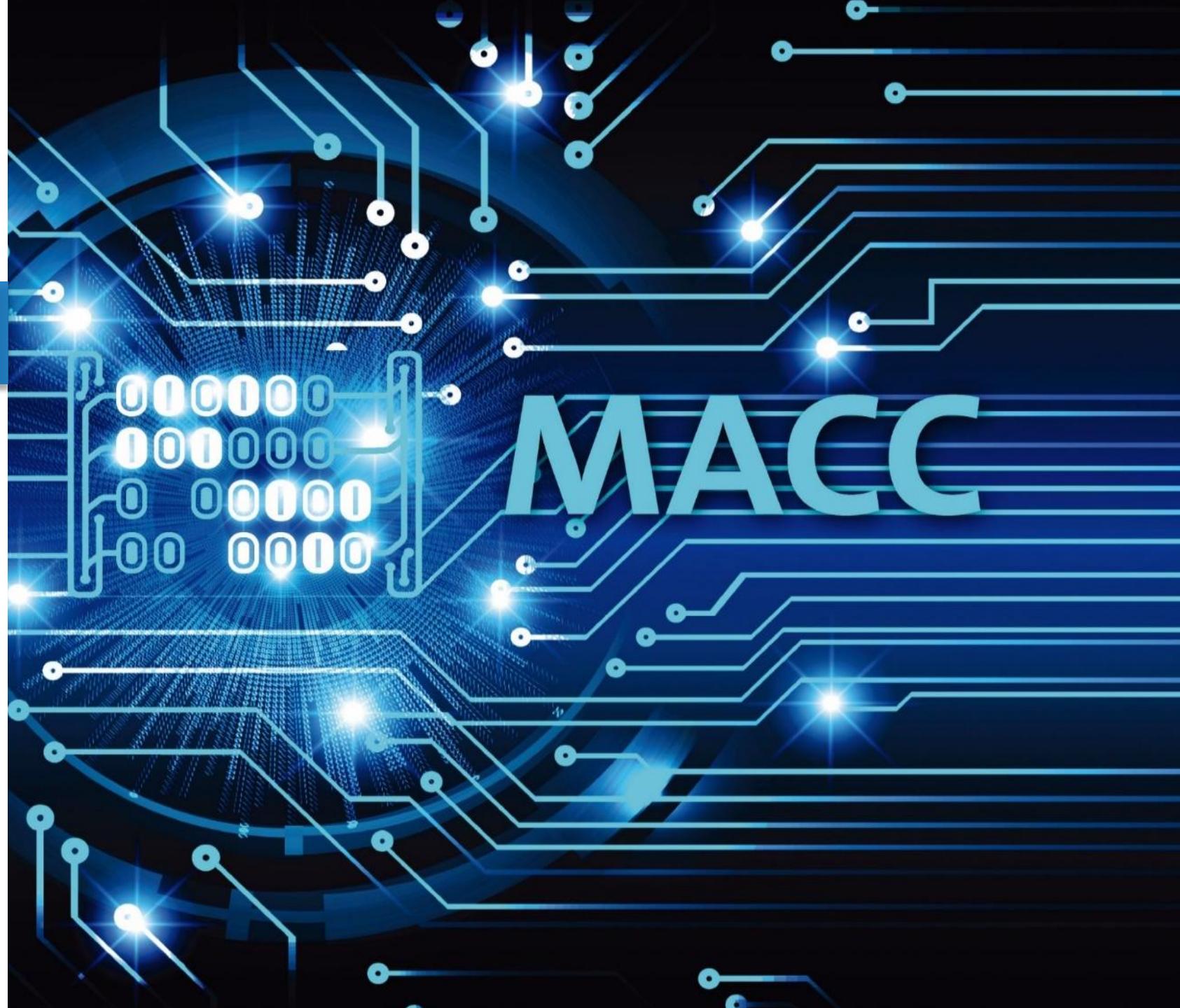
MACC  
Matemáticas Aplicadas y  
Ciencias de la Computación

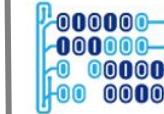
## Wireless Networks

Hacking Ético

Daniel Orlando Díaz López, PhD

Profesor principal  
Departamento MACC  
Universidad del Rosario  
[danielo.diaz@urosario.edu.co](mailto: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)

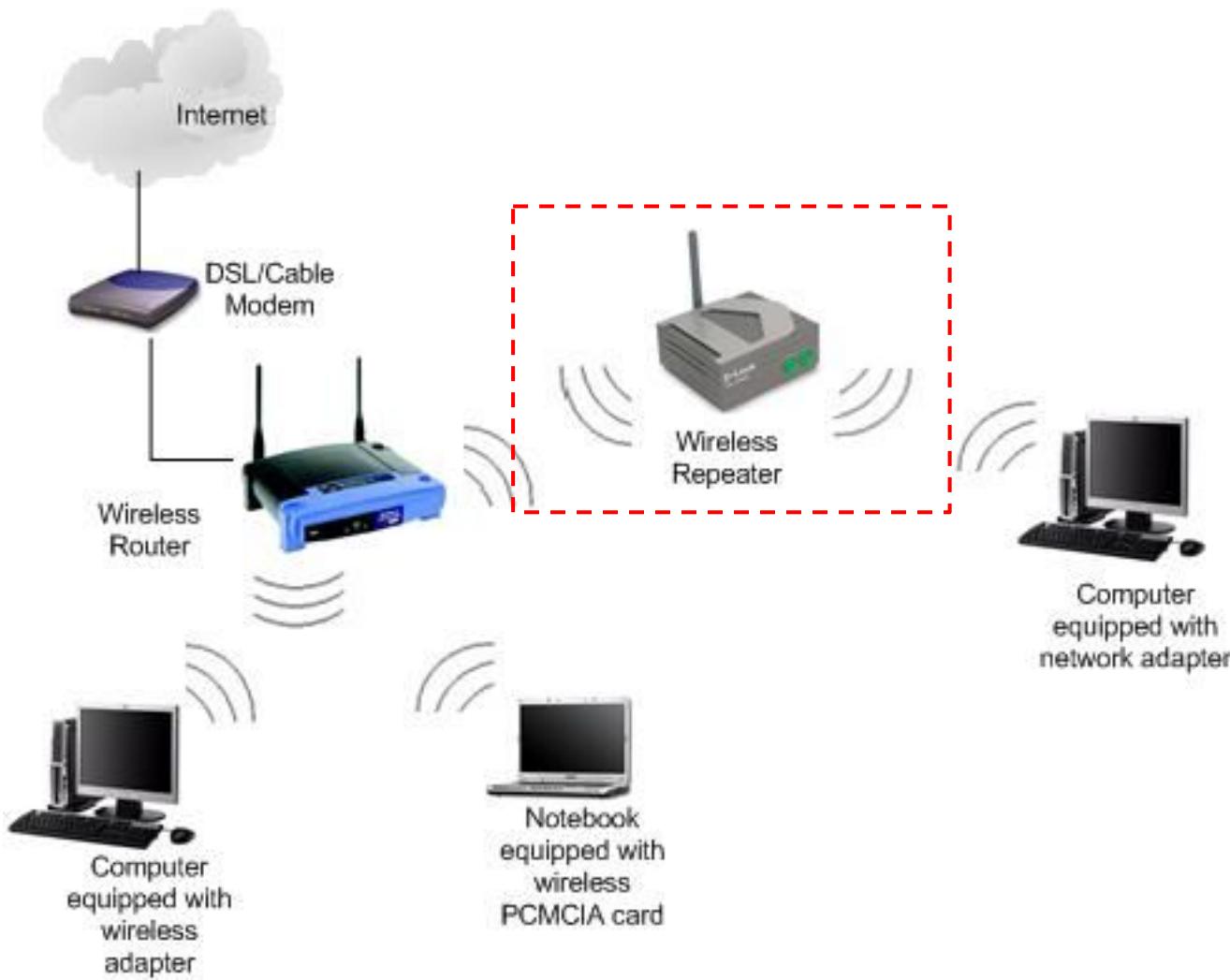
**BSSID:** Es la dirección MAC de un Access Point / Router inalámbrico

**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

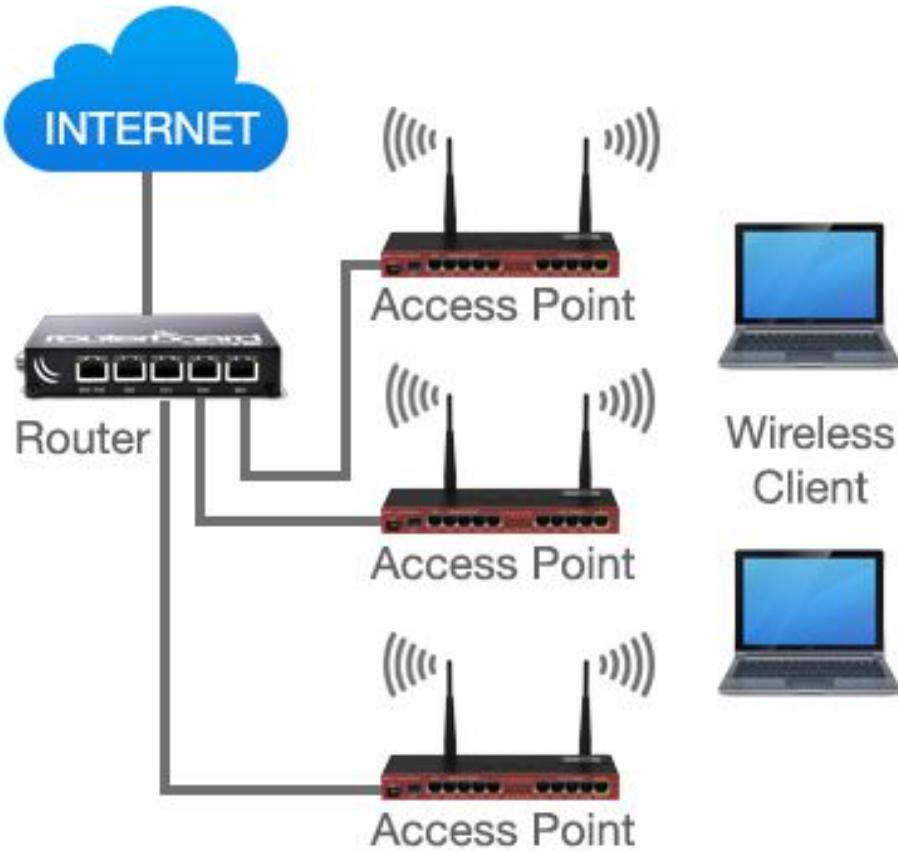
**Hotspot:** lugar en el cual se dispone de servicio de red inalámbrica

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

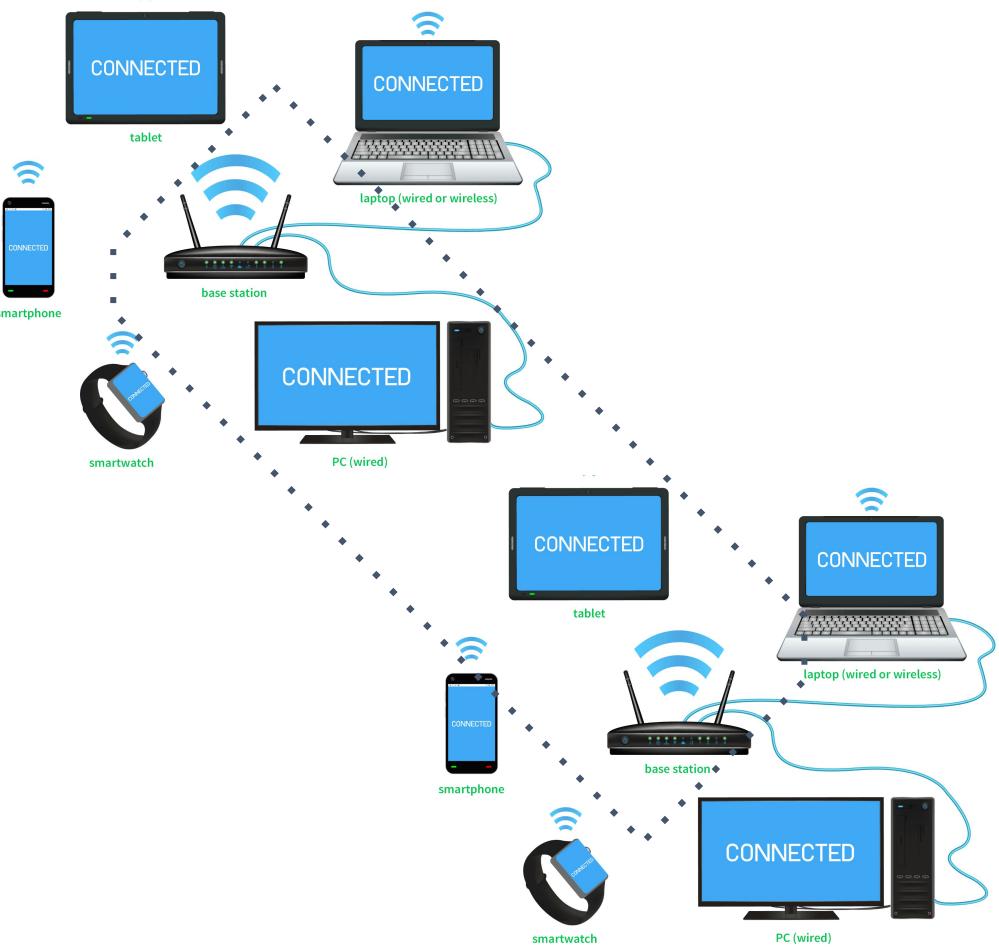


But it here!

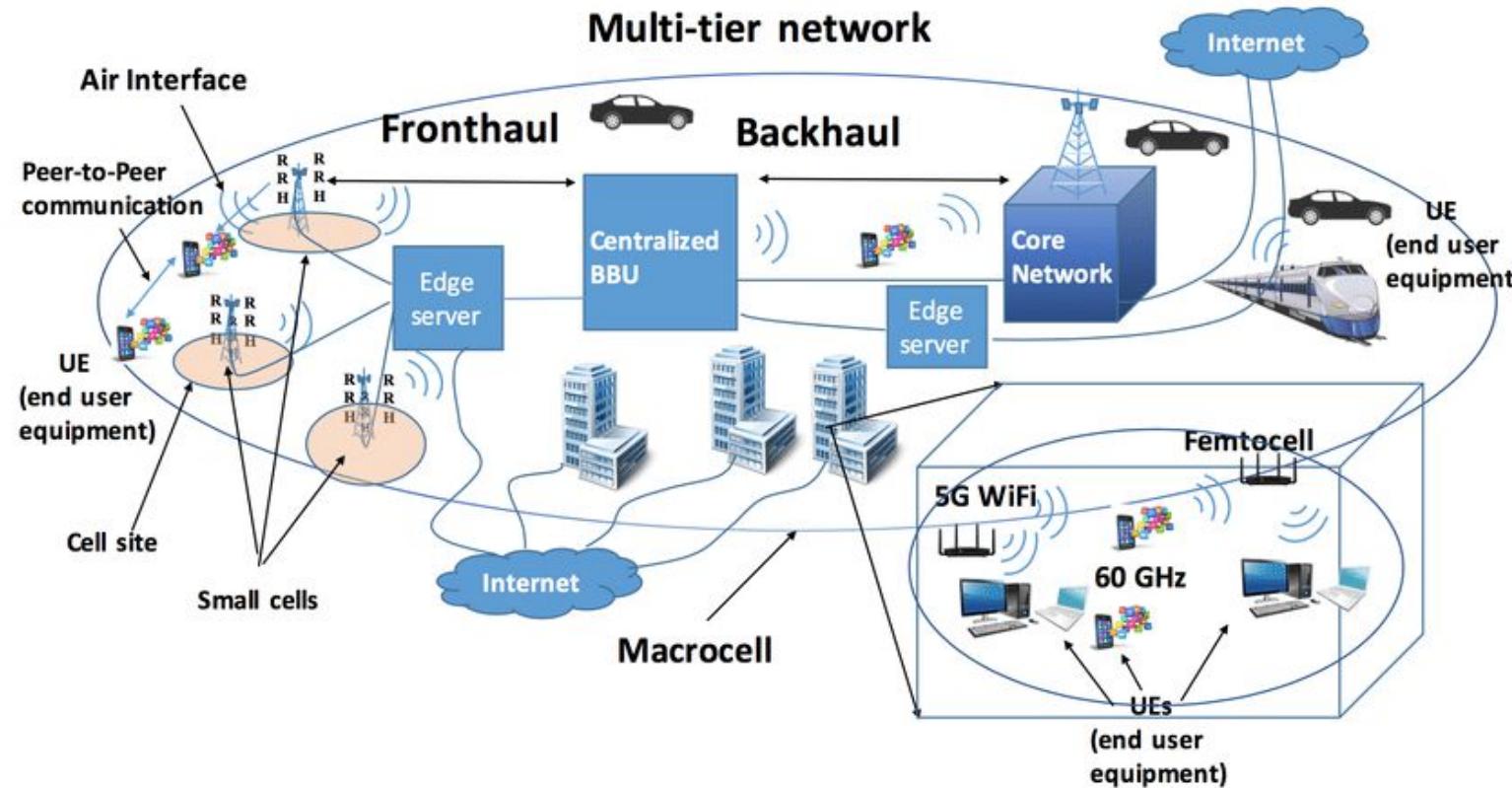
### 2. Múltiples APs desplegados y sirviendo el mismo SSID



### 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

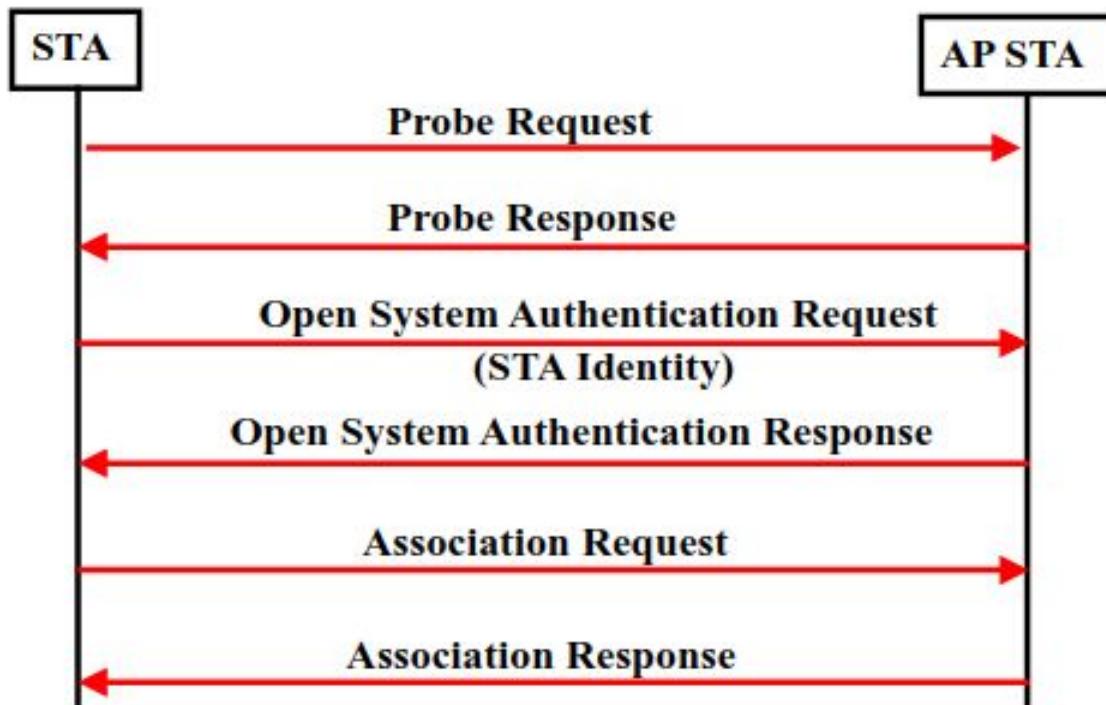
Bandwidth vs Range

Battery life vs Bandwidth



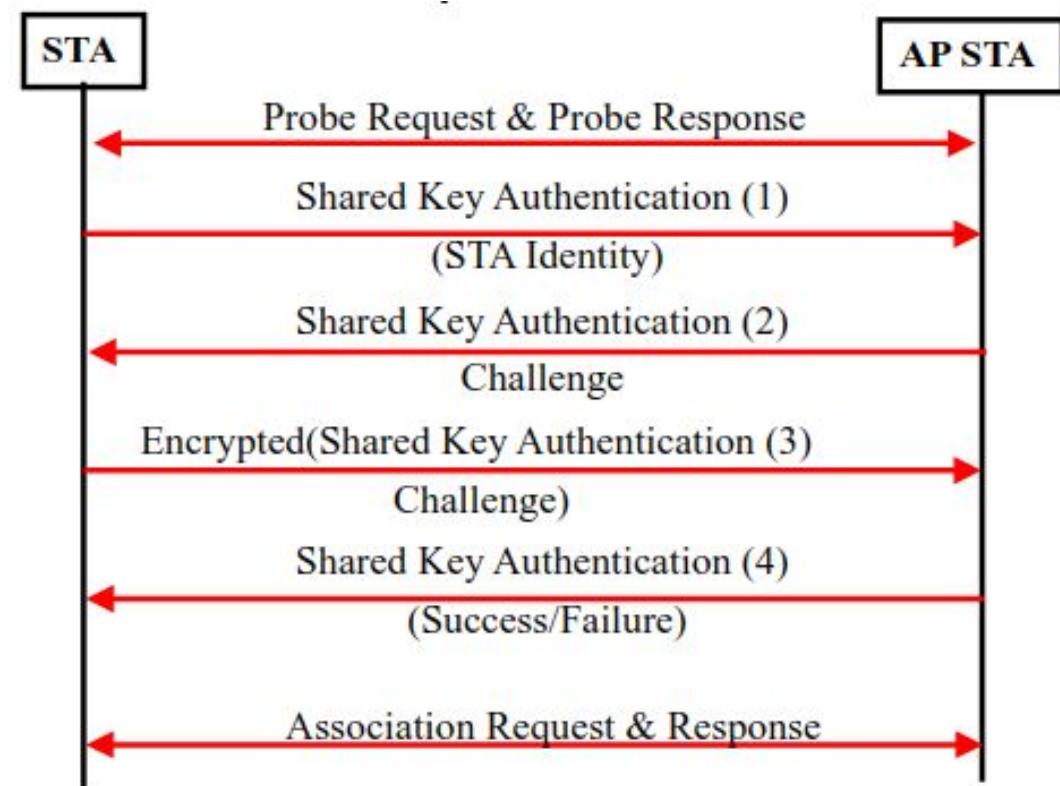
## Redes con autenticación abierta

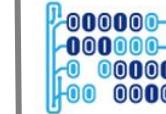
Ejemplos: Restaurantes, Aeropuertos, puntos Vive Digital, etc



## Redes con autenticación de llave compartida tipo WEP

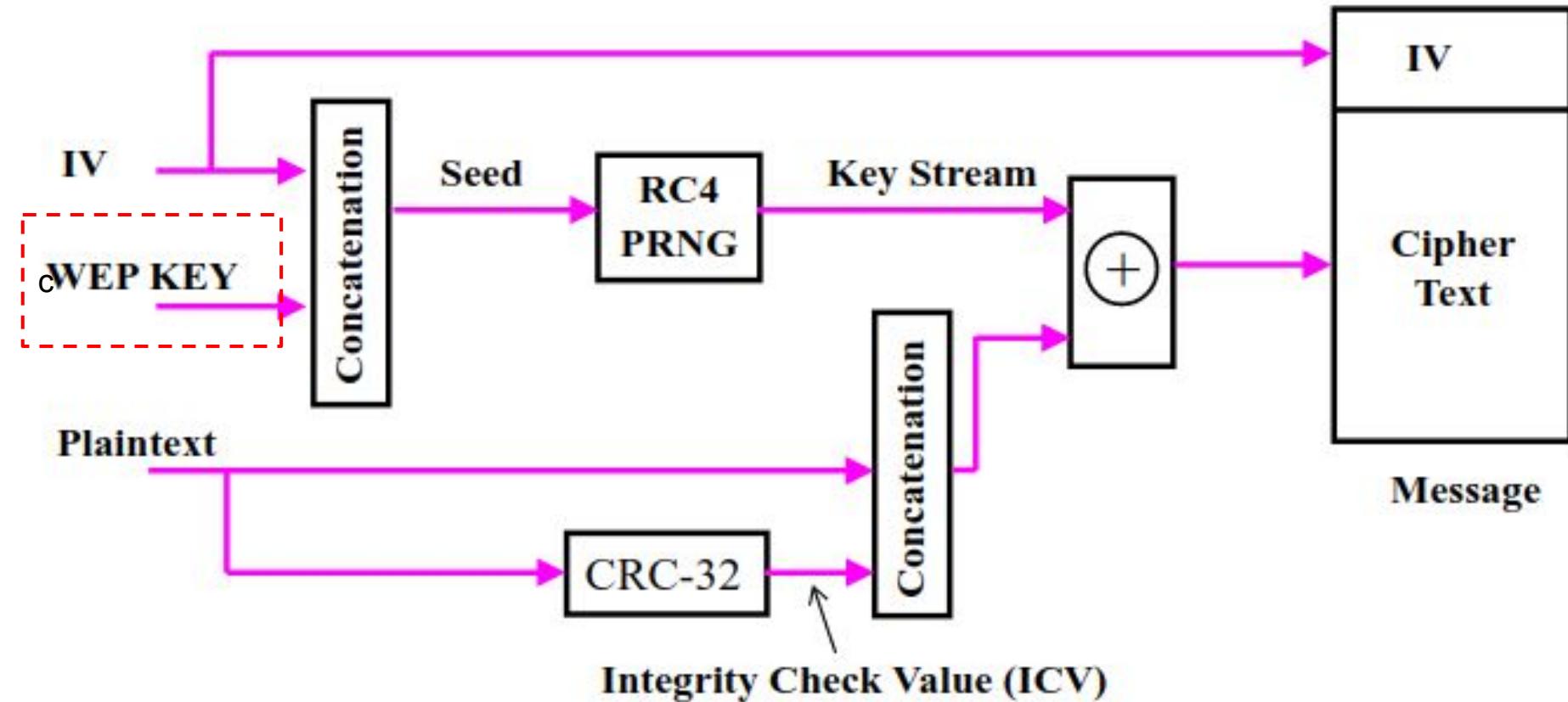
Ejemplos: Red inalámbrica de hogar, algunas oficinas, etc

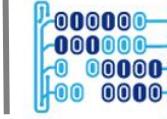




WEP (Wired Equivalent Privacy) utiliza el algoritmo de cifrado RC4

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



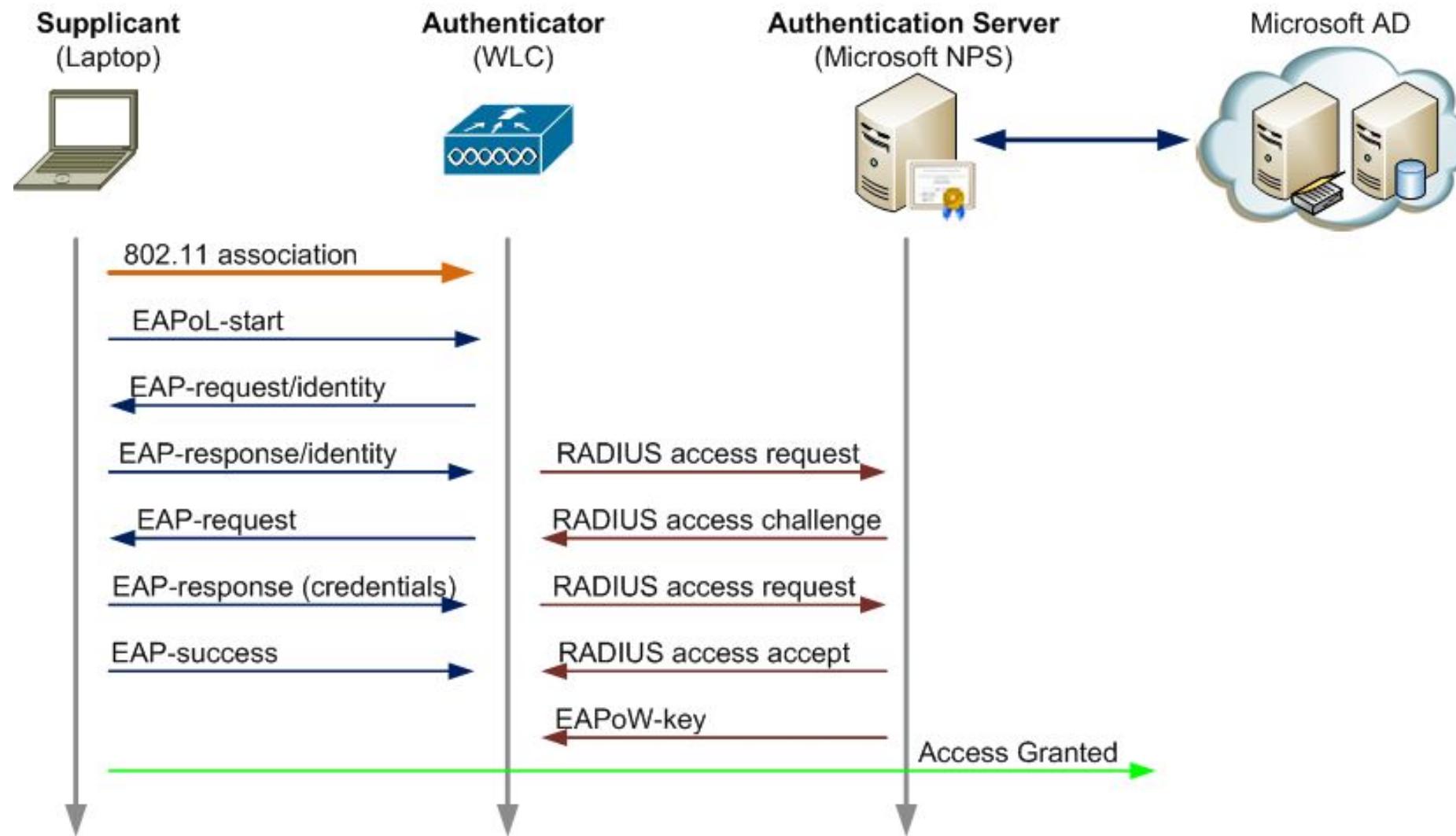
## Wifi Authentication Modes



	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 cipher 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!

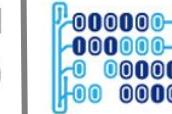
## Autenticación utilizando un servidor de autenticación





## Tipos de ataques a redes inalámbricas

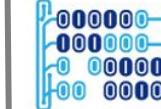
Network Layer	Security Attack	Countermeasure
Physical	Jamming Tampering	Spread-spectrum, frequency hopping Tamper-proof design
Link	Collisions Exhaustion Unfairness	Error-correcting codes Data rate limits, time division multiplexing Short frames
Network and Routing	Spoofing, altering, replaying Sinkholes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



## Realizar diferentes tipos de ataques a una red inalámbrica

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

C kali.org/downloads/

**KALI**  
BY OFFENSIVE SECURITY  
concurrent connections.

Blog Downloads Training Documentation

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](#)



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!

```
urosario@CNP77151: ~
File Edit View Search Terminal Help
(base) urosario@CNP77151:~$ echo "deb https://deb.etcher.io stable etcher" | sudo tee /etc/apt/sources.list.d/balena-etcher.list

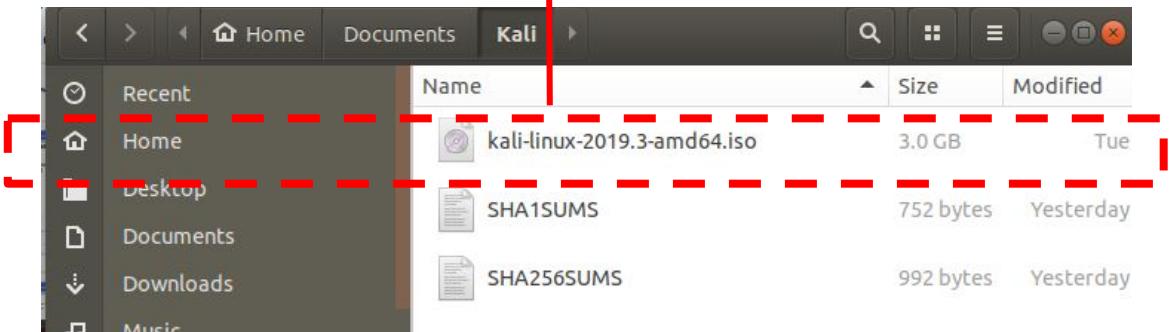
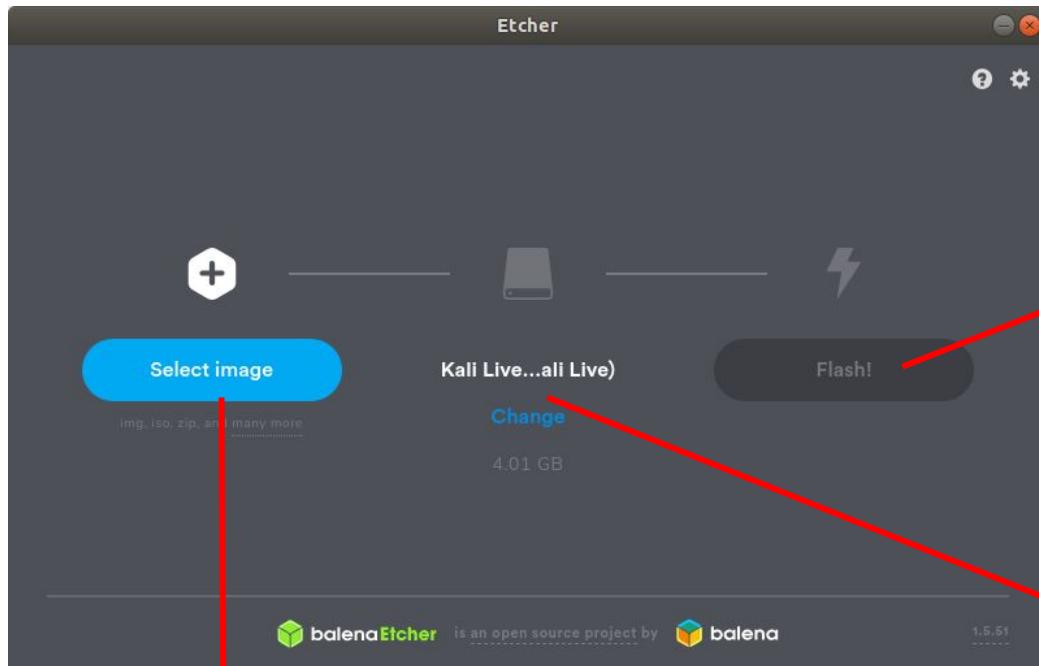
(base) urosario@CNP77151:~$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 379CE192D401AB61

(base) urosario@CNP77151:~$ sudo apt-get update

(base) urosario@CNP77151:~$ sudo apt-get install balena-etcher-electron

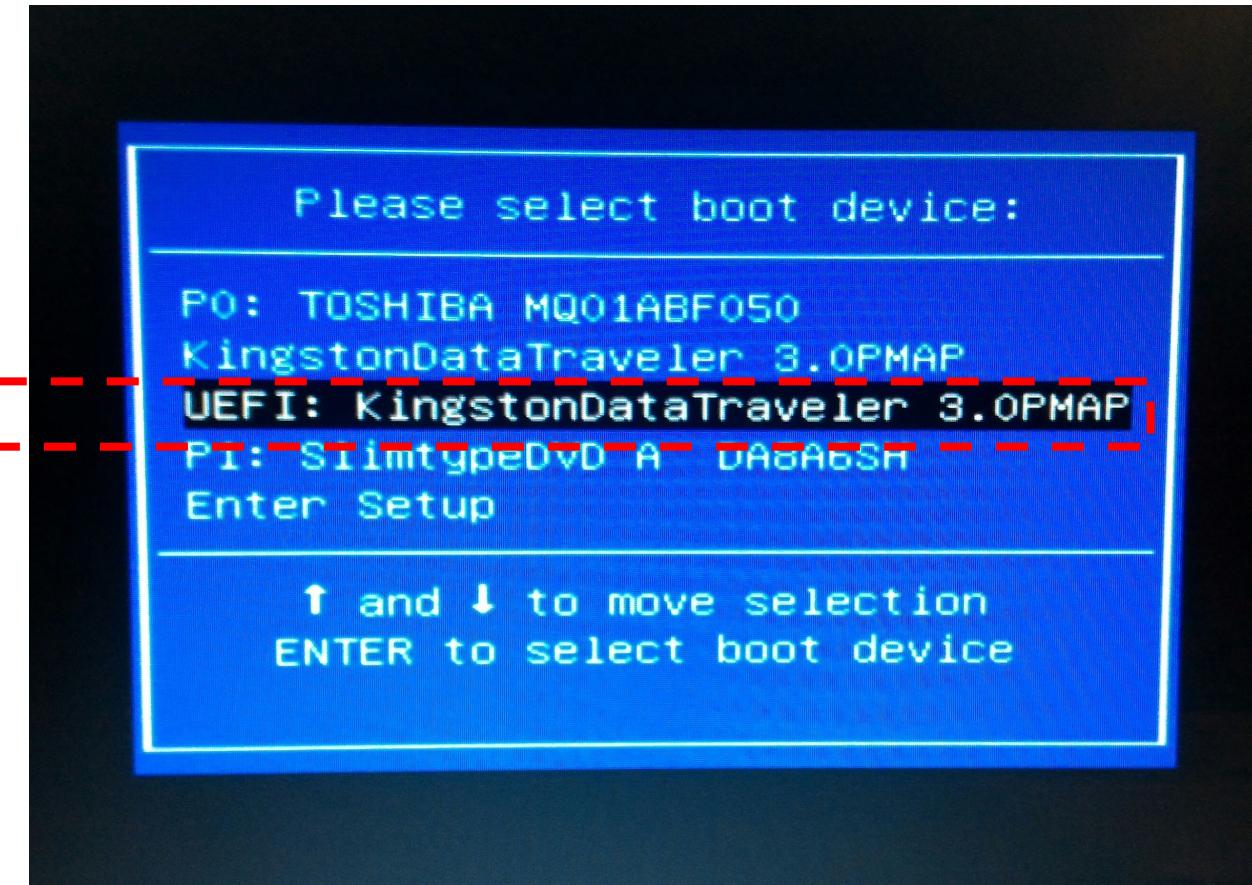
(base) urosario@CNP77151:~$ balena-etcher-electron
```

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>

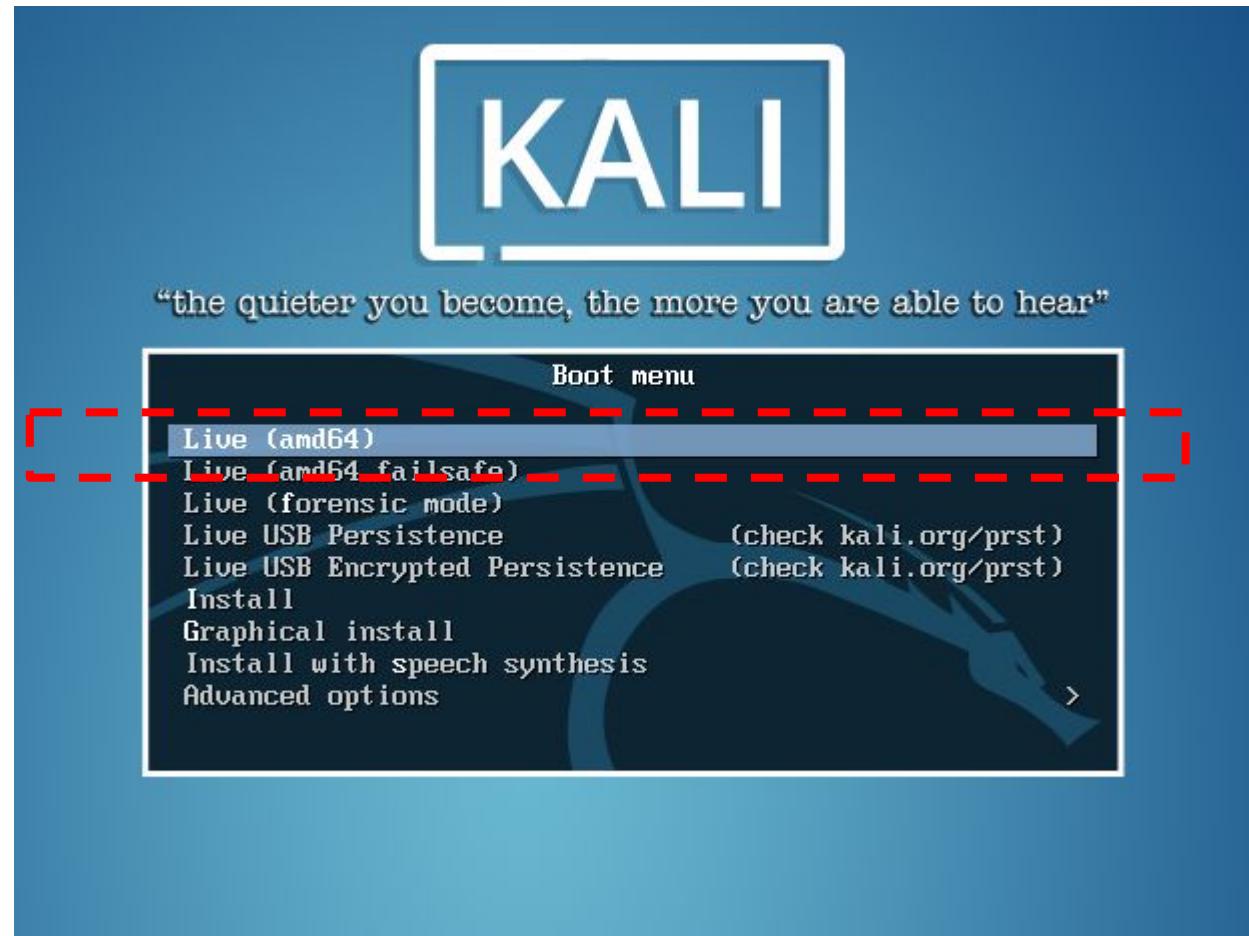


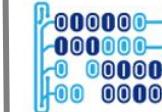
Continue

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!





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>

root@kali:/usr/bin# kismet

```
root@kali: ~
File Edit View Search Terminal Help
KISMET - Point your browser to http://localhost:2501 for the Kismet UI
INFO: Did not find a user plugin directory (/root/.kismet/plugins/),
      skipping: No such file or directory
INFO: GPS track will be logged to the Kismet logfile
INFO: Enabling channel hopping by default on sources which support channel
      control.
INFO: Setting default channel hop rate to 5/sec
INFO: Enabling channel list splitting on sources which share the same list
      of channels
INFO: Enabling channel list shuffling to optimize overlaps
INFO: Sources will be re-opened if they encounter an error
INFO: Saving datasources to the Kismet database log every 30 seconds.
INFO: Launching remote capture server on 127.0.0.1:3501
INFO: No data sources defined; Kismet will not capture anything until a
      source is added.
INFO: Opened kismetdb log file './Kismet-20191031-17-20-25-1.kismet'
INFO: Saving packets to the Kismet database log.
ALERT: rootuser Kismet is running as root; this is less secure. If you
      are running Kismet at boot via systemd, make sure to use `systemctl
      edit kismet.service` to change the user. For more information, see
      the Kismet README for setting up Kismet with minimal privileges.
INFO: Starting Kismet web server...
INFO: Started http server on port 2501
```

# Acceso web a la interfaz de kismet



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

Applications ▾ Places ▾ Firefox ESR ▾

Thu 17:20

Kismet - Mozilla Firefox

localhost:2501/devices/bx | +

localhost:2501

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

29% 2h 37m

Kismet

Wi-Fi Access Points

Name Type Phy Crypto Signal Channel Last Seen Data Packets Clients BSSID QBSS Chan Usage QBSS Users

No data available in table

0 devices

Messages Channels

Current Historical Past Minute Filter Any Frequency

1.0  
0.5  
0

60 55 50 45 40 35 30 25 20 15 10 5

Powered by many OSS components, see the [credits page](#)

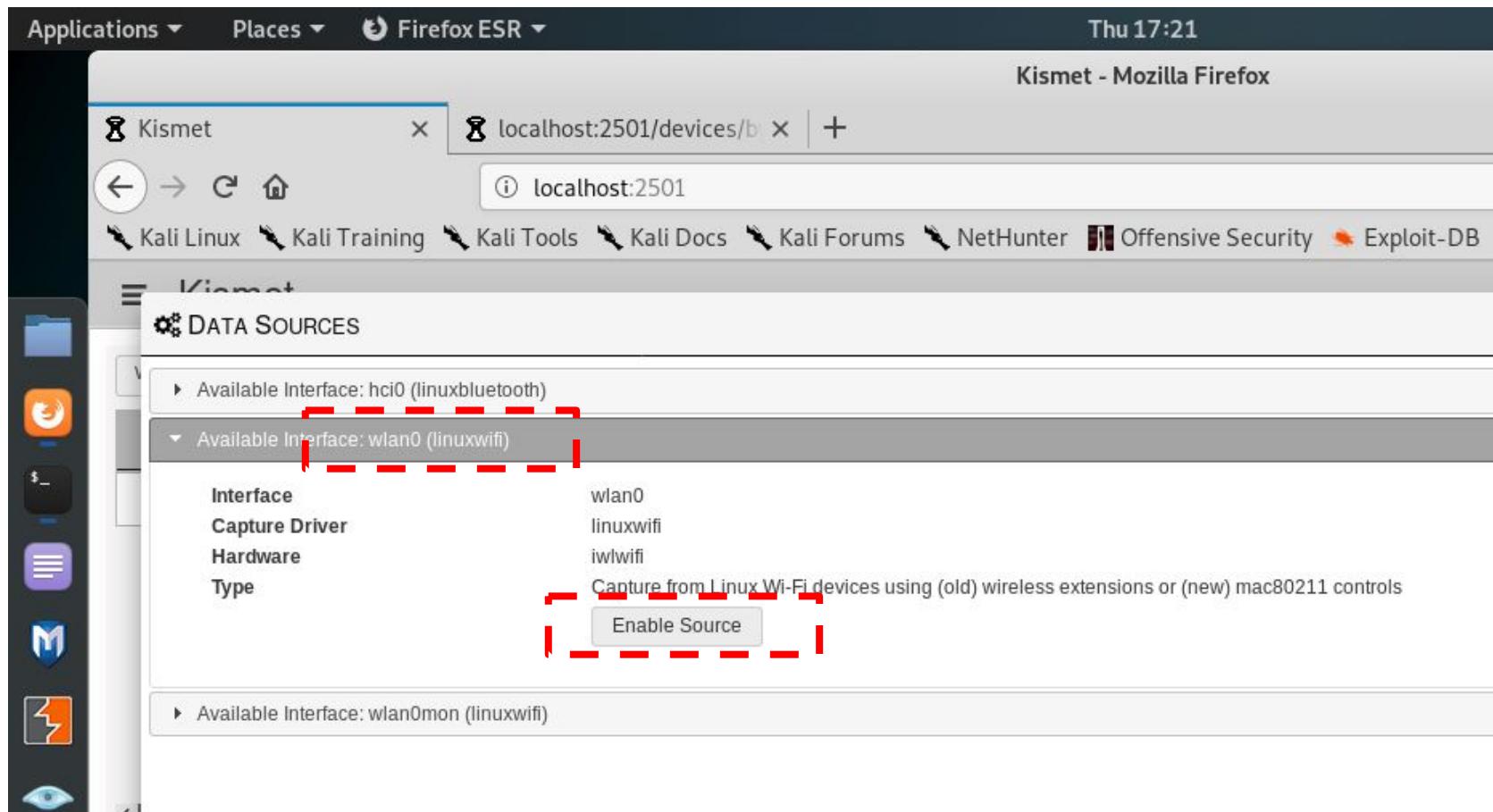
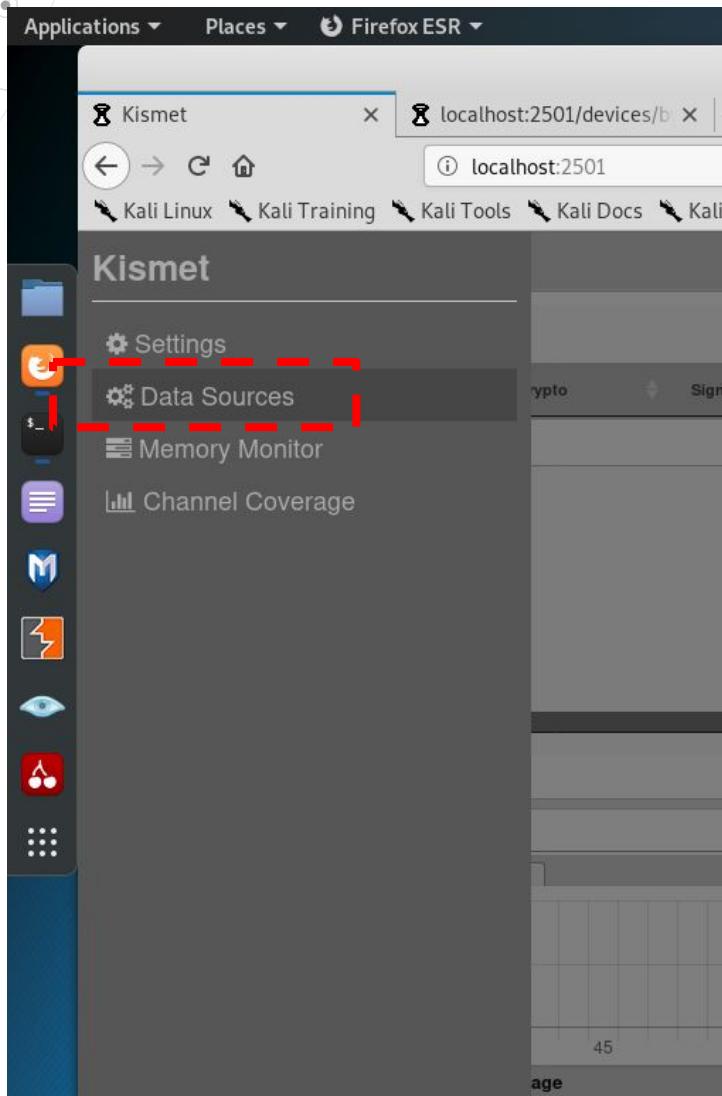
# Habilitación de la fuente de datos para Kismet



Universidad del  
**Rosario**



**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación



## Redes inalámbricas detectadas por kismet



Universidad del  
**Rosario**

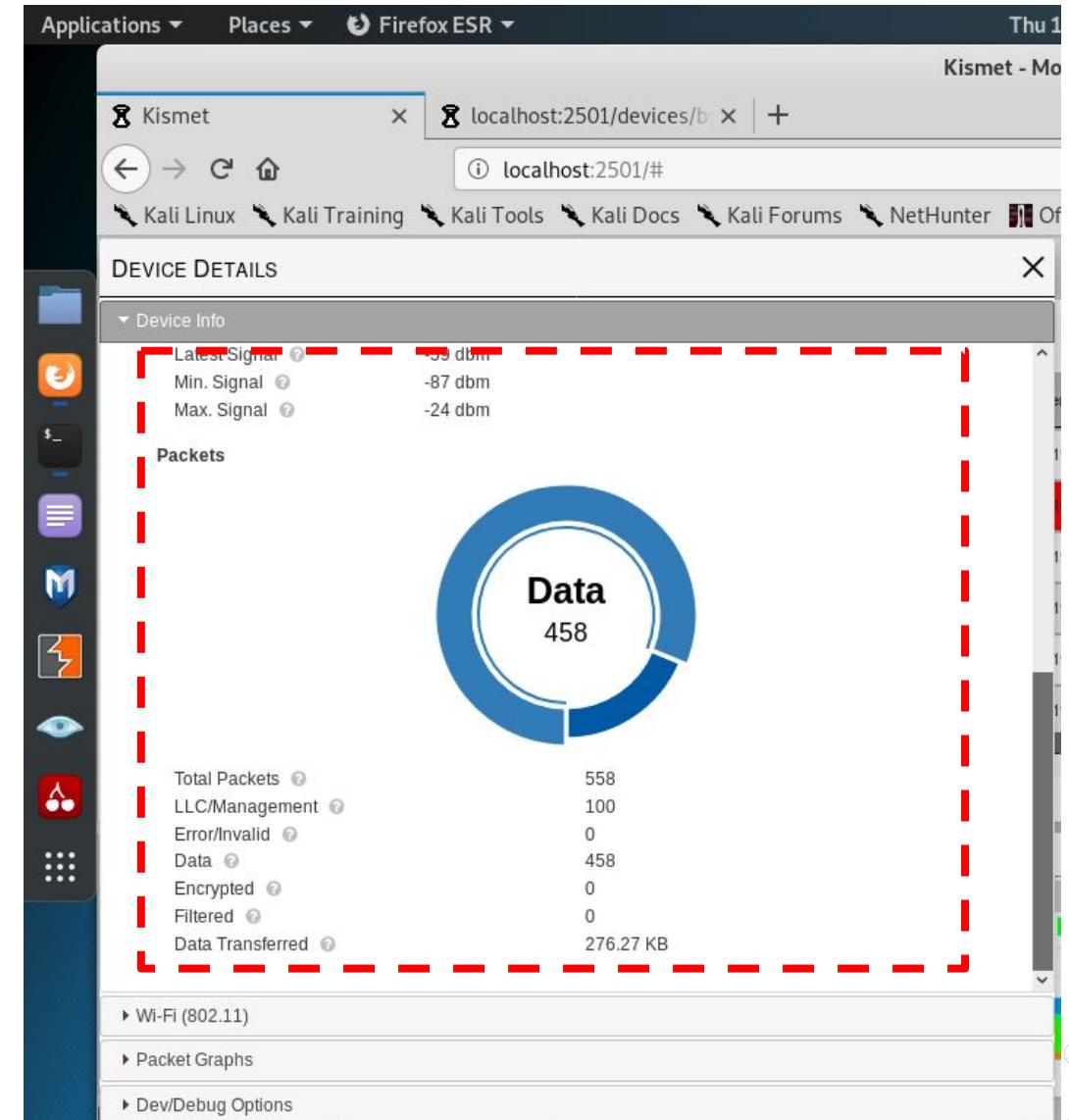
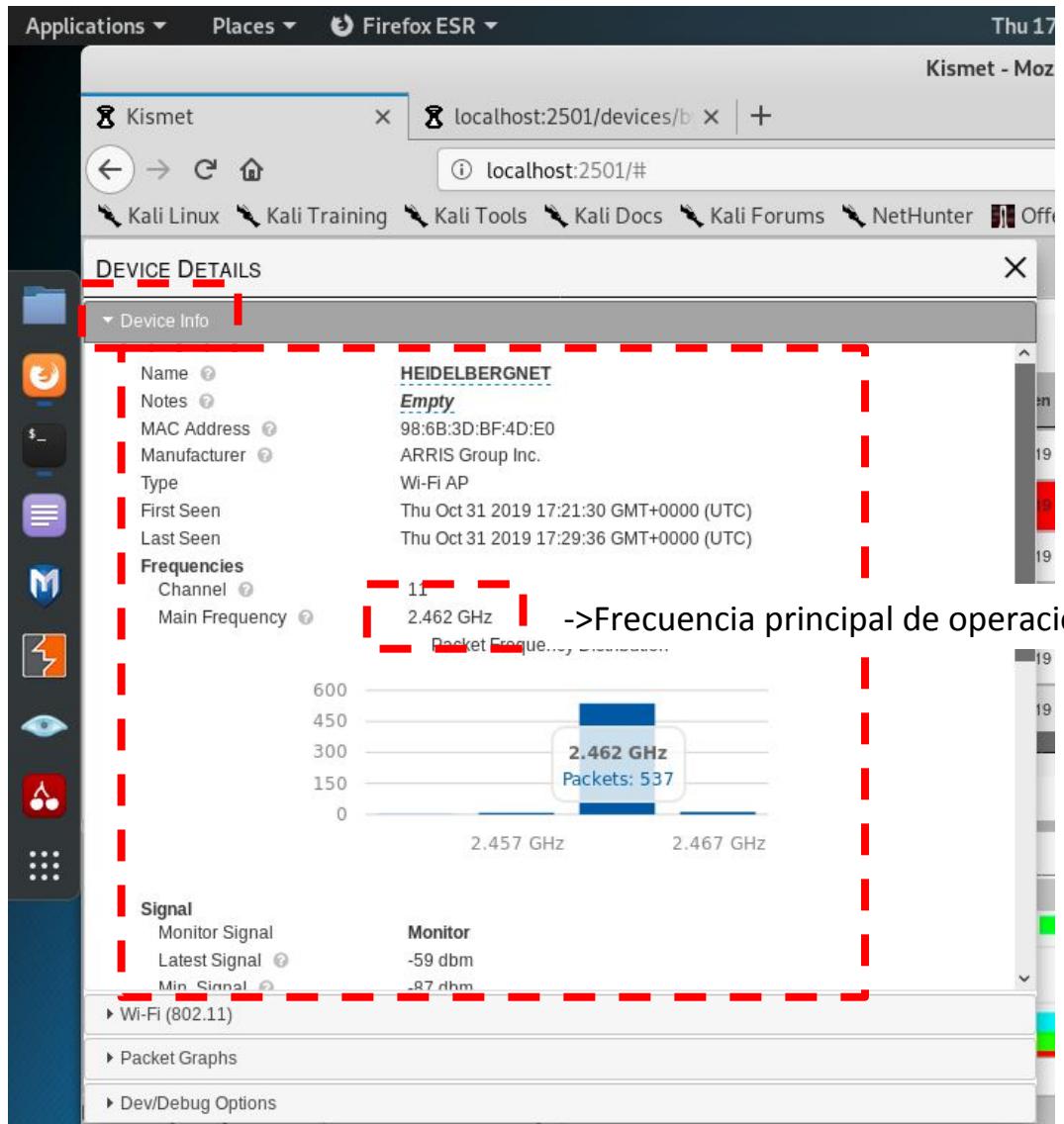


**MACC**  
Matemáticas Aplicadas y  
Ciencias de la Computación

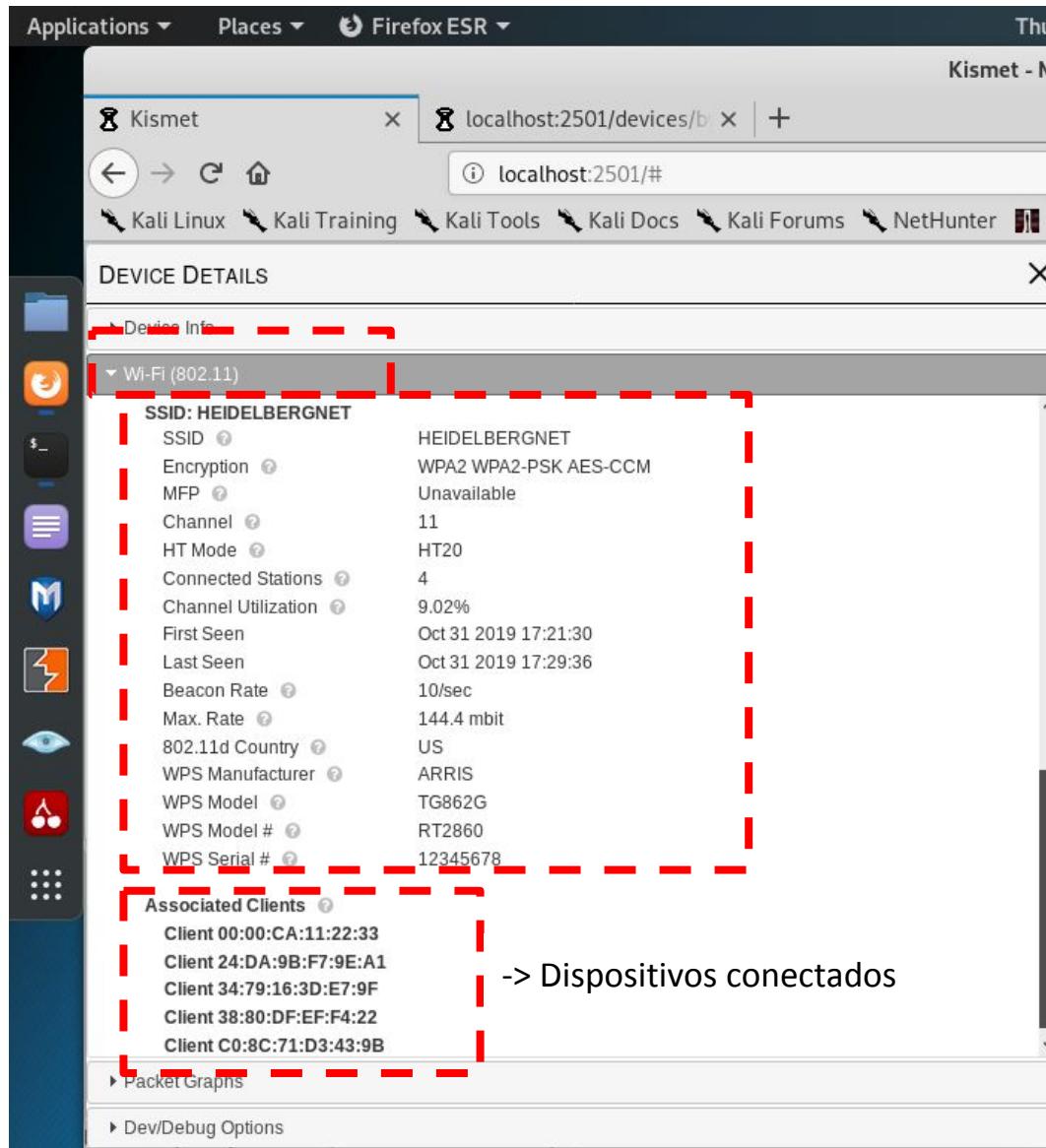
The screenshot shows the Kismet web interface running in Mozilla Firefox. The title bar indicates it's running on Thu 17:21. The main content area displays a table of detected Wi-Fi access points. The table has columns for Name, Type, Phy, Crypto, Signal, Channel, Last Seen, Data, Packets, Clients, BSSID, QBSS Chan Usage, and QBSS Users. A dropdown menu above the table is set to 'Wi-Fi Access Points'. The table lists several access points, including HEIDELBERGNET, HITRON-EC60, Mayra Pinzon, 46:32:C8:C6:D4:19, FAMILIA\_RATIVA, and ESLAVA C. Each row includes a small bar chart representing signal strength and usage. The bottom section of the interface shows a 'Messages' log and a 'Channels' section.

Name	Type	Phy	Crypto	Signal	Channel	Last Seen	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS Users
HEIDELBERGNET	Wi-Fi AP	IEEE802.11	WPA2-PSK	-64	11	Oct 31 2019 17:21:44	0 B	.....█..	0	98:6B:3D:BF:4D:E0	12.16%	3
HITRON-EC60	Wi-Fi AP	IEEE802.11	WPA2-PSK	-79	11	Oct 31 2019 17:21:40	0 B	.....█..	0	F0:F2:49:35:EC:68	16.47%	3
Mayra Pinzon	Wi-Fi AP	IEEE802.11	WPA2-PSK	-81	1	Oct 31 2019 17:21:34	7.42 KB	.....█..	2	90:0D:CB:B3:D7:00	48.24%	3
46:32:C8:C6:D4:19	Wi-Fi AP	IEEE802.11	WPA2-PSK	-82	6	Oct 31 2019 17:21:44	0 B	.....█..	0	46:32:C8:C6:D4:19	n/a	n/a
FAMILIA_RATIVA	Wi-Fi AP	IEEE802.11	WPA2-PSK	-83	6	Oct 31 2019 17:21:44	0 B	.....█..	0	AC:84:C6:75:34:2C	n/a	n/a
ESLAVA C	Wi-Fi AP	IEEE802.11	WPA2-PSK	-84	6	Oct 31 2019 17:21:44	0 B	.....█..	0	44:32:C8:C6:D4:18	n/a	n/a

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



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



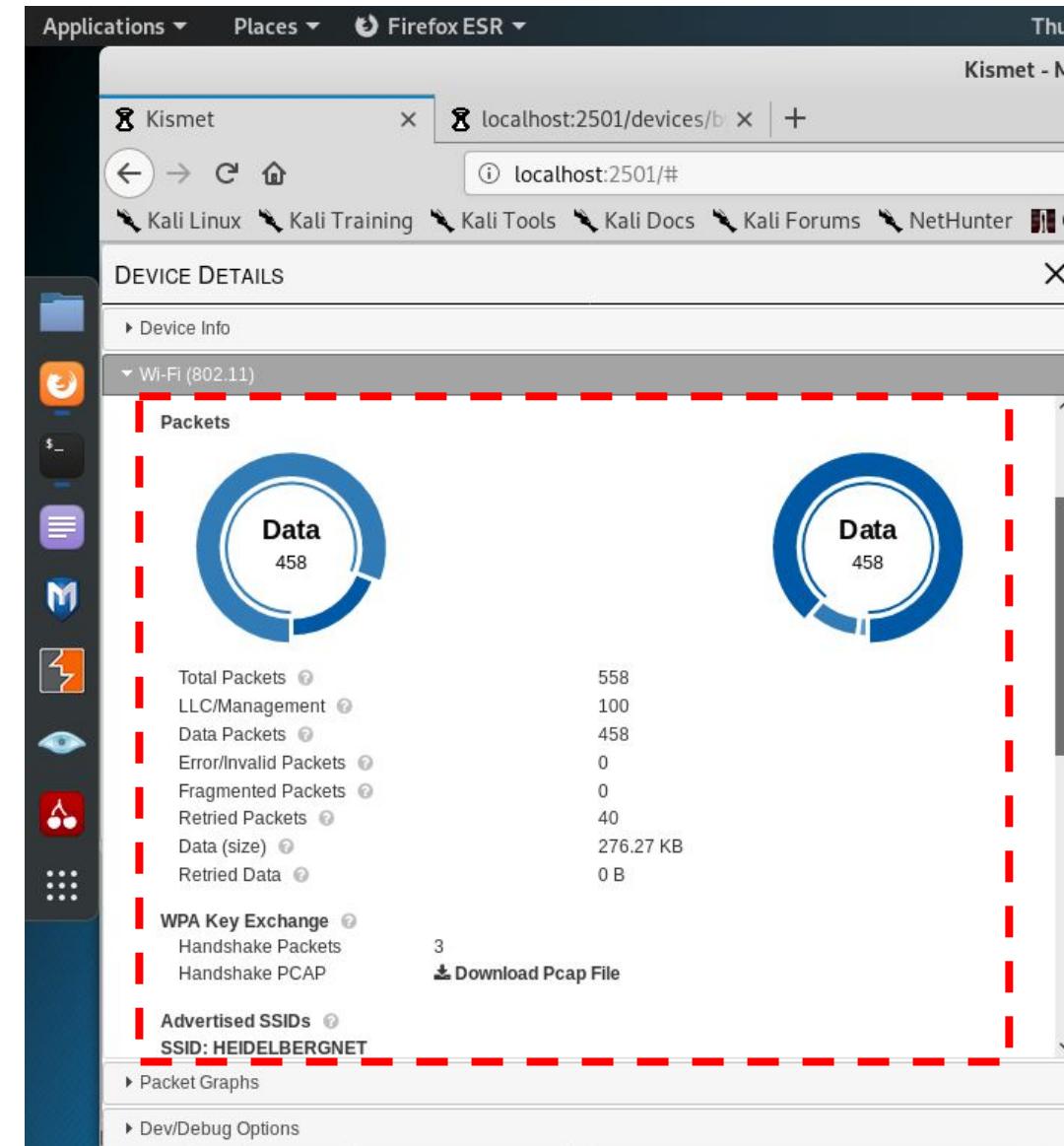
The screenshot shows the Kismet interface with the title "Kismet - Monitors". The main window displays "DEVICE DETAILS" for the SSID "HEIDECKERNET". The "Wi-Fi (802.11)" section provides the following information:

Parameter	Value
SSID	HEIDECKERNET
Encryption	WPA2 WPA2-PSK AES-CCM
MFP	Unavailable
Channel	11
HT Mode	HT20
Connected Stations	4
Channel Utilization	9.02%
First Seen	Oct 31 2019 17:21:30
Last Seen	Oct 31 2019 17:29:36
Beacon Rate	10/sec
Max. Rate	144.4 mbit
802.11d Country	US
WPS Manufacturer	ARRIS
WPS Model	TG862G
WPS Model #	RT2860
WPS Serial #	12345678

The "Associated Clients" section lists five connected devices:

- Client 00:00:CA:11:22:33
- Client 24:DA:9B:F7:9E:A1
- Client 34:79:16:3D:E7:9F
- Client 38:80:DF:EF:F4:22
- Client C0:8C:71:D3:43:9B

A red dashed box highlights the "Associated Clients" section, and an arrow points from it to the text "-> Dispositivos conectados".



The screenshot shows the Kismet interface with the title "Kismet - Monitors". The main window displays "DEVICE DETAILS" for the SSID "HEIDECKERNET". The "Packets" section provides the following data:

Category	Value
Total Packets	558
LLC/Management	100
Data Packets	458
Error/Invalid Packets	0
Fragmented Packets	0
Retried Packets	40
Data (size)	276.27 KB
Retried Data	0 B

The "WPA Key Exchange" section shows 3 handshake packets and a link to "Download Pcap File". The "Advertised SSIDs" section lists "SSID: HEIDECKERNET".

Kismet - Mozilla Firefox

Thu 17:31

1 es

Kismet

localhost:2501/devices/b

localhost:2501/#

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

DEVICE DETAILS

Device Info

Wi-Fi (802.11)

Data 458

Total Packets 558

LLC/Management 100

Data Packets 458

Error/Invalid Packets 0

Fragmented Packets 0

Retried Packets 40

Data (size) 276.27 KB

Retried Data 0 B

WPA Key Exchange 3

Handshake Packets 3

Handshake PCAP Download Pcap File

Advertised SSIDs HEIDELBERGNET

SSID HEIDELBERGNET

Encryption WPA2 WPA2-PSK AES-CCM

MFP Unavailable

Channel 11

HT Mode HT20

Packet Graphs

Dev/Debug Options

Opening 4202770D00000000\_E04DBF3D6B980000-handshake.pcap

You have chosen to open:

4202770D00000000\_E04DBF3D6B980000-handshake.pcap

which is: Packet Capture (PCAP) (786 bytes)

from: http://localhost:2501

What should Firefox do with this file?

Open with Wireshark (default)

Save File

Do this automatically for files like this from now on.

Cancel OK

Clients BSSID QBSS Chan Usage QBSS

4 90:0D:CB:B3:D7:00 41.96% 3

5 98:6B:3D:BF:4D:E0 9.412% 4

4 F0:F2:49:35:EC:68 17.65% 3

1 44:32:C8:C6:D4:18 n/a n/a

1 34:21:09:58:7E:C1 16.47% 1

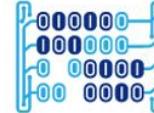
1 80:C6:AB:57:C4:68 n/a n/a

Frequency 2.447 GHz 2.452 GHz 2.457 GHz 2.462 GHz 2.467 GHz 5.180 GHz 5.640 GHz

# 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

Applications ▾ Places ▾ Wireshark ▾ Thu 17:33

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ArrisGro_bf:4d:e0	Broadcast	802.11	277	Beacon frame, SN=2408, FN=0, Flags=....., BI=100, SSID=HEIDELB...
2	-0.033319	ArrisGro_bf:4d:e0	Motorola_d3:43:9b	EAPOL	133	Key (Message 1 of 4)
3	-0.031710	ArrisGro_bf:4d:e0	Motorola_d3:43:9b	EAPOL	133	Key (Message 1 of 4)
4	0.009940	Motorola_d3:43:9b	ArrisGro_bf:4d:e0	EAPOL	155	Key (Message 2 of 4)

...0 ..... = Encrypted Key Data: Not set  
..0. .... = SMK Message: Not set  
Key Length: 16  
Replay Counter: 1  
WPA Key Nonce: 27aafa5687e8729009fe4179ec8fe7e8bf2cfdf51f83de96b...  
Key IV: 00000000000000000000000000000000  
WPA Key RSC: 0000000000000000  
WPA Key ID: 0000000000000000  
WPA Key MIC: 00000000000000000000000000000000  
WPA Key Data Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
0000	88 02 ca 00 c0 8c 71 d3 43 9b 98 6b 3d bf 4d e0				.....q.C.k=M.	
0010	98 6b 3d bf 4d e0 00 00 00 00 aa aa 03 00 00 00				.k=M.....	
0020	88 8e 01 03 00 5f 02 00 8a 00 10 00 00 00 00 00				'..V..r..Ay..	
0030	00 00 01 27 aa fa 56 87 e8 72 90 09 fe 41 79 ec				,Q.=k..0	
0040	8f e7 e8 bf 2c fd 51 f8 3d e9 6b de 8d b4 a0 51					
0050	de 96 ef 00 00 00 00 00 00 00 00 00 00 00 00 00					
0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					

WPA Key Nonce (wlan\_rsna\_eapol.keydes.nonce), 32 bytes

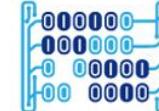
Packets: 4 · Displayed: 4 (100.0%)

Profile: Default

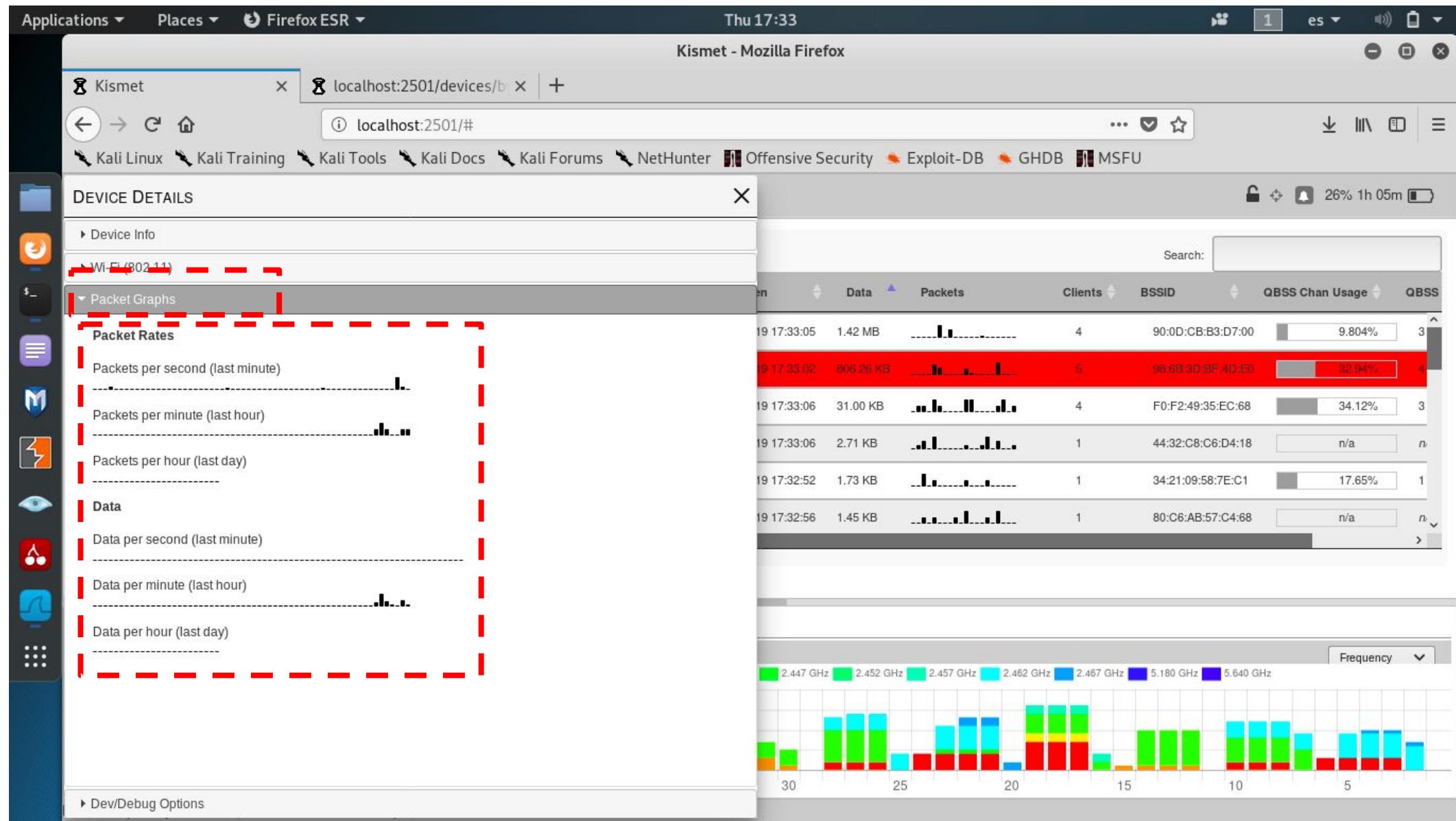
Acceso a la sección “Packet Graphs” de una de las redes detectadas (Heidelbergnet)

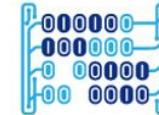


Universidad del  
Rosario



MACC  
Matemáticas Aplicadas y  
Ciencias de la Computación





Applications ▾ Places ▾ Firefox ESR ▾

Thu 17:33

Kismet - Mozilla Firefox

localhost:2501/devices/b | +

localhost:2501/#

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

**Kismet**

Wi-Fi Access Points

Name	Type	Phy	Crypto	Signal	Channel	Last Seen	Data
Mayra Pinzon	Wi-Fi AP	IEEE802.11	WPA2-PSK	-78	1	Oct 31 2019 17:33:19	1.42 MB
HEIDELBERGNET	Wi-Fi AP	IEEE802.11	WPA2-PSK	-66	11	Oct 31 2019 17:33:20	807.76 KB
HITRON-EC60	Wi-Fi AP	IEEE802.11	WPA2-PSK	-80	11	Oct 31 2019 17:33:20	31.20 KB
ESLAVA C	Wi-Fi AP	IEEE802.11	WPA2-PSK	-91	6	Oct 31 2019 17:33:15	2.71 KB
Familia echeverry	Wi-Fi AP	IEEE802.11	WPA2-PSK	-87	6	Oct 31 2019 17:33:15	1.73 KB
FAMILIA ESTEVEZ	Wi-Fi AP	IEEE802.11	WPA2-PSK	-80	2	Oct 31 2019 17:33:15	1.45 KB

46 devices

Messages Channels

Current Past Minute Filter Any

2.412 GHz 2.417 GHz 2.422 GHz 2.427 GHz 2.432 GHz 2.437 GHz 2.442 GHz 2.447 GHz 2.452 GHz 2.457 GHz 2.462 GHz 2.467 GHz 2.467 GHz 5.180 GHz 5.640 GHz

Showing all alerts...

Alerts

Oct 31 2019 17:20:25 rootuser

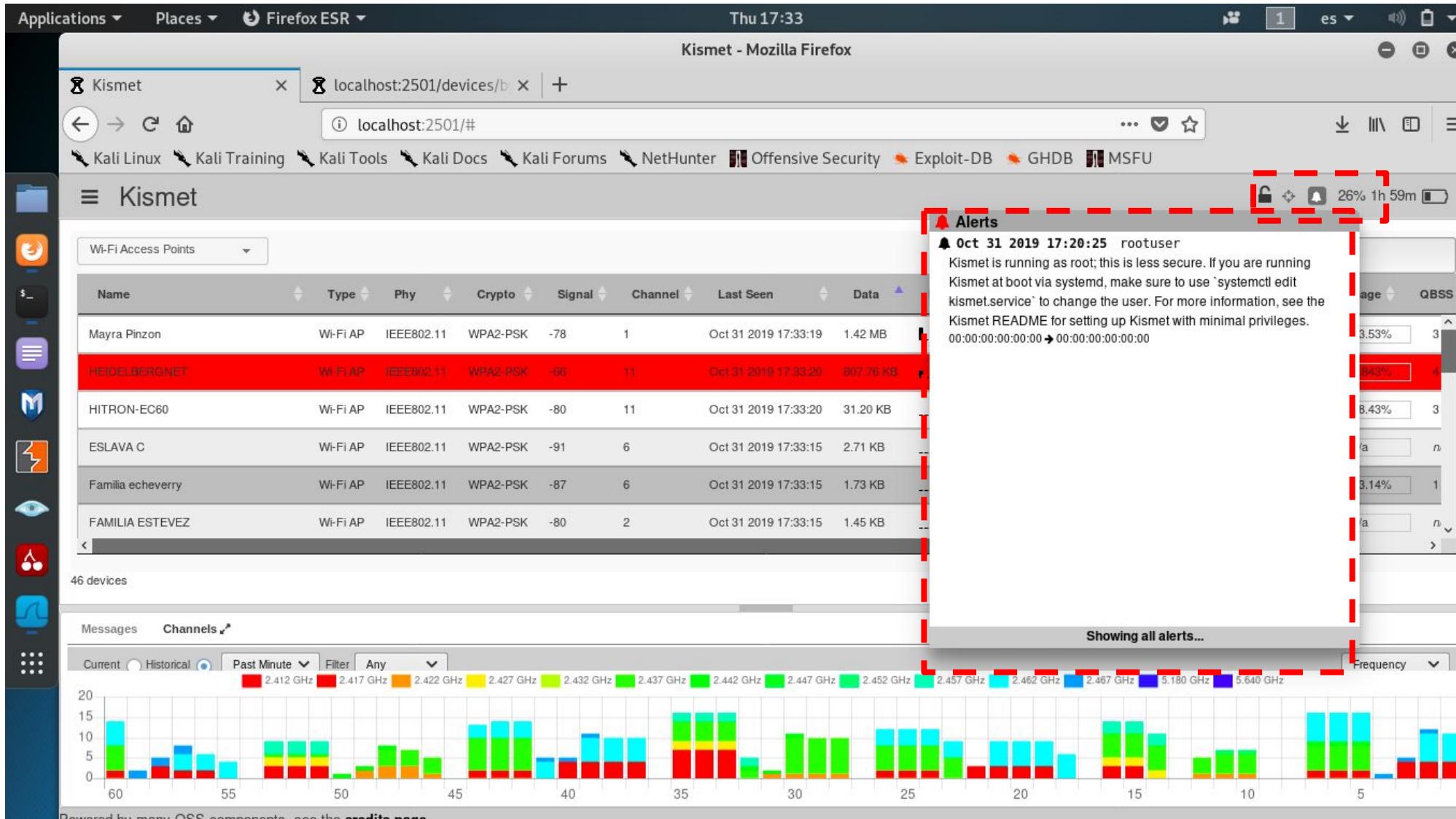
Kismet is running as root; this is less secure. If you are running Kismet at boot via systemd, make sure to use `systemctl edit kismet.service` to change the user. For more information, see the Kismet README for setting up Kismet with minimal privileges.

00:00:00:00:00 → 00:00:00:00:00

age QBSS

3.53% 3 84.3% 4 8.43% 3 /a n 3.14% 1 /a n >

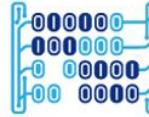
Powered by many OSS components, see the [credits page](#)



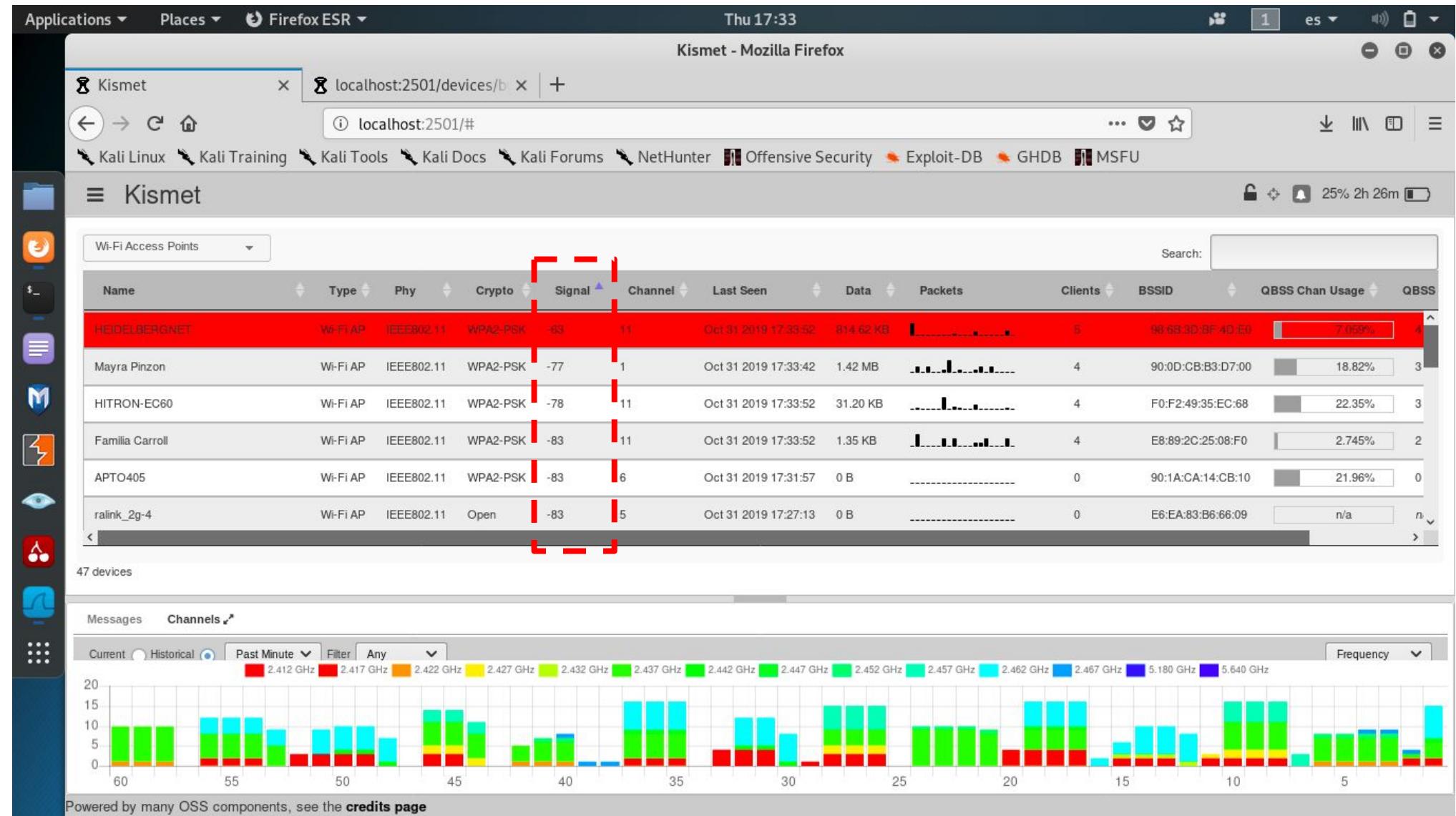
# Ordenación de redes por nivel de señal (Mayor a menor)



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

Applications ▾ Places ▾ Firefox ESR ▾

Thu 17:34

Kismet - Mozilla Firefox

Kismet localhost:2501/devices/b +  
localhost:2501/#

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

☰ Kismet

Wi-Fi Access Points

Name	Type	Phy	Crypto	Signal	Channel	Last Seen	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS
ralink_2g-4	Wi-Fi AP	IEEE802.11	Open	-83	5	Oct 31 2019 17:27:13	0 B	-----	0	E6:EA:83:B6:66:09	n/a	n/a
Mayra Pinzon	Wi-Fi AP	IEEE802.11	WPA2-PSK	-76	1	Oct 31 2019 17:34:00	1.42 MB	███████	4	90:0D:CB:B3:D7:00	6.667%	3
CARDESCO	Wi-Fi AP	IEEE802.11	WPA2-PSK	-91	1	Oct 31 2019 17:34:00	1.28 KB	██████	2	54:A6:19:4C:B6:60	n/a	n/a
FAMILIA MENESSES	Wi-Fi AP	IEEE802.11	WPA2-PSK	-92	4	Oct 31 2019 17:34:00	794 B	██████	3	94:87:7C:60:13:E0	5.882%	4
FAMILIA_RATIVA	Wi-Fi AP	IEEE802.11	WPA2-PSK	-90	6	Oct 31 2019 17:34:10	0 B	███████	2	AC:84:C6:75:34:2C	n/a	n/a
ESLAVA C	Wi-Fi AP	IEEE802.11	WPA2-PSK	-91	6	Oct 31 2019 17:34:10	2.71 KB	██████████	1	44:32:C8:C6:D4:18	n/a	n/a

47 devices

Messages Channels

Current Historical Past Minute Filter Any Frequency

2.412 GHz 2.417 GHz 2.422 GHz 2.427 GHz 2.432 GHz 2.437 GHz 2.442 GHz 2.447 GHz 2.452 GHz 2.457 GHz 2.462 GHz 2.467 GHz 2.472 GHz 5.180 GHz 5.640 GHz

Powered by many OSS components, see the [credits page](#)

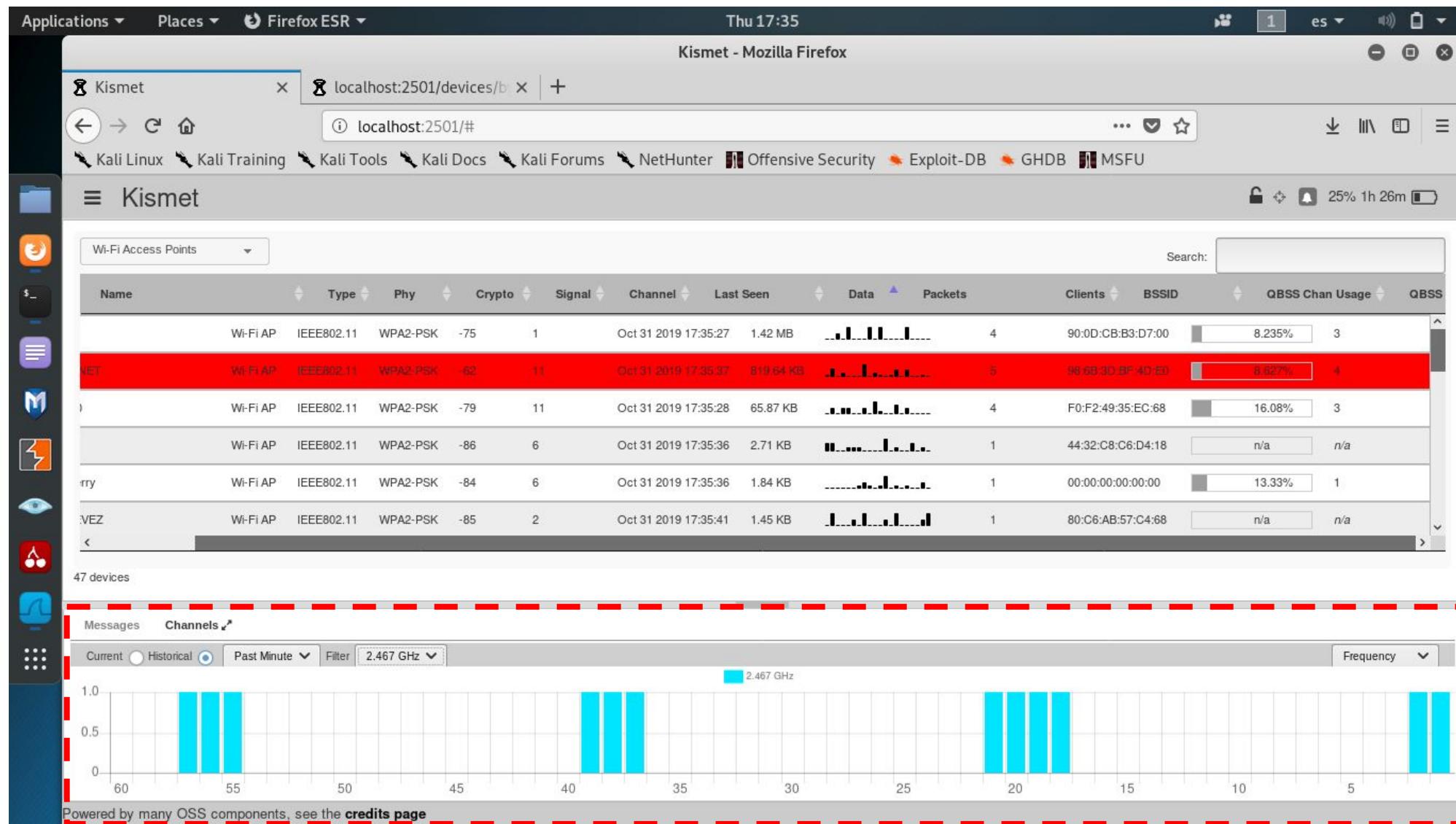
Dispositivos transmitiendo en la frecuencia 2.46 Ghz



Universidad del  
Rosario



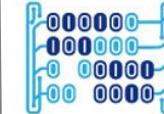
MACC  
Matemáticas Aplicadas y  
Ciencias de la Computación



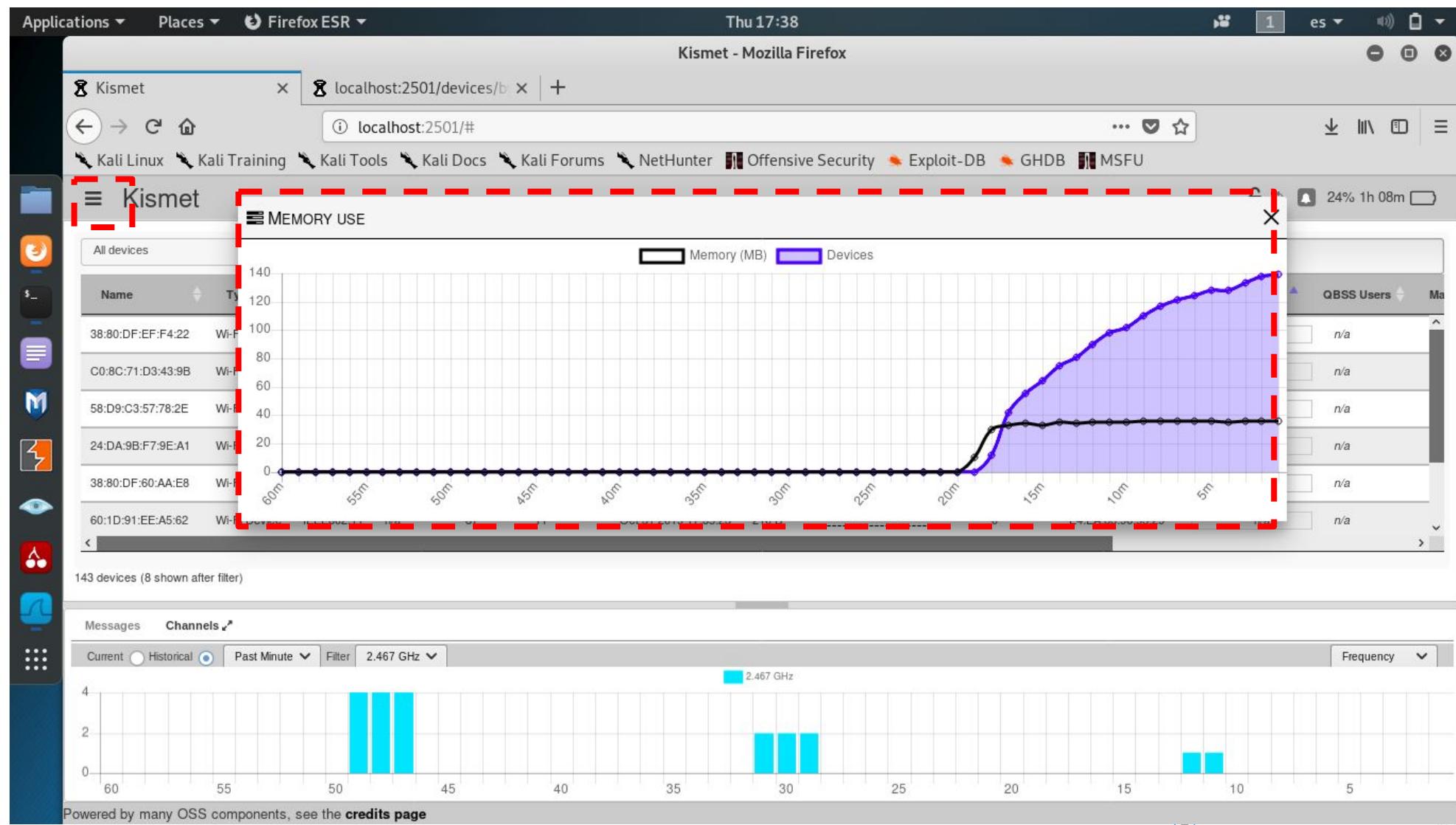
# Número de dispositivos detectados por kismet y consumo de RAM por parte de Kismet



Universidad del  
Rosario



MACC  
Matemáticas Aplicadas y  
Ciencias de la Computación



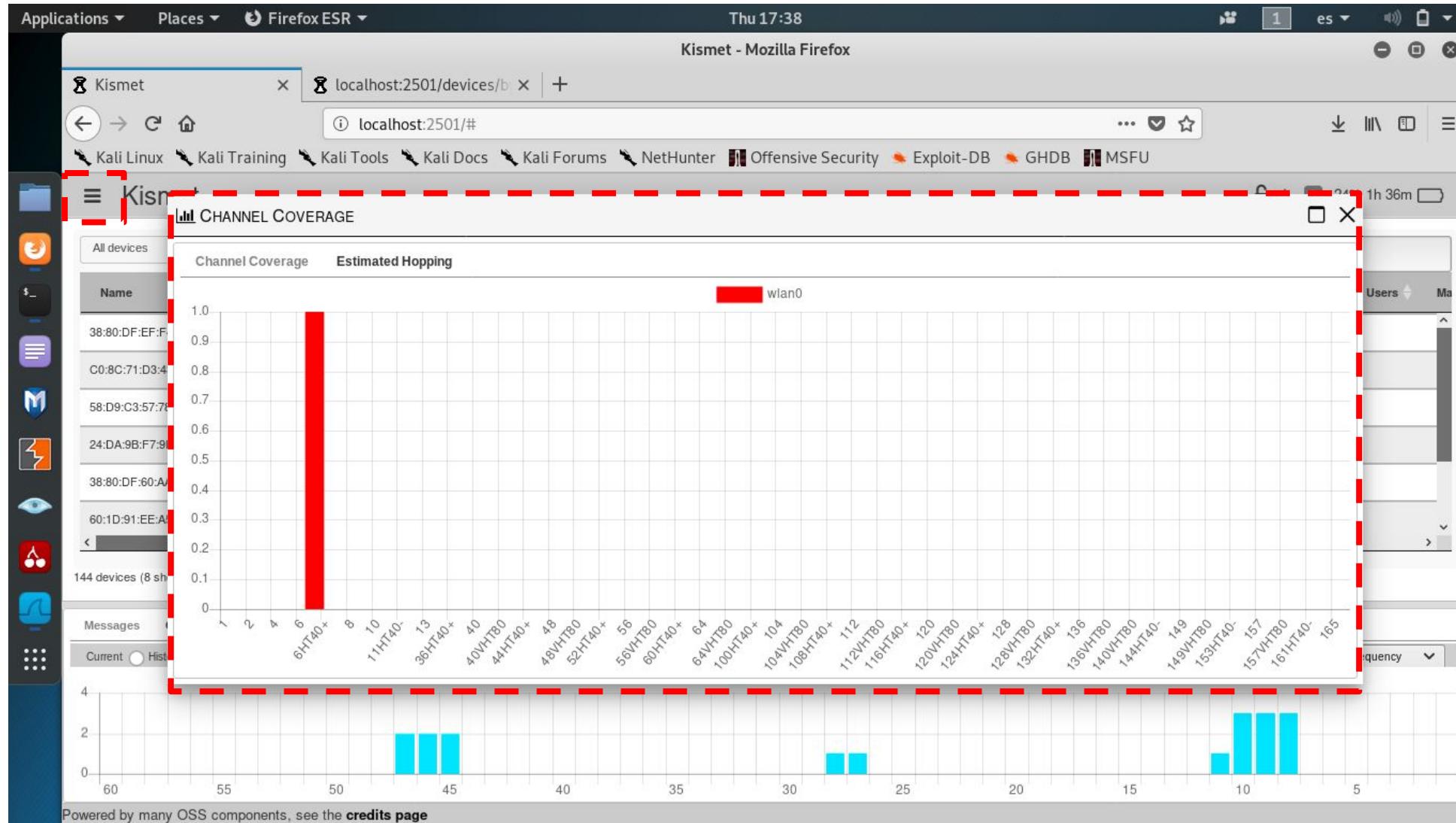
Salto de frecuencia realizado por Kismet para poder detectar dispositivos en diferentes frecuencias

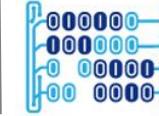


Universidad del  
Rosario



MACC  
Matemáticas Aplicadas y  
Ciencias de la Computación





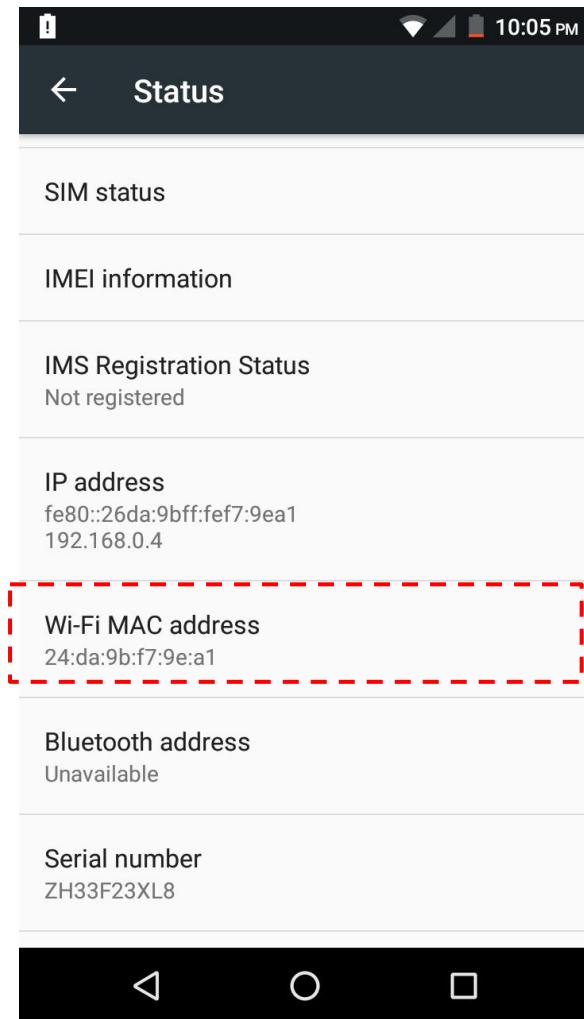
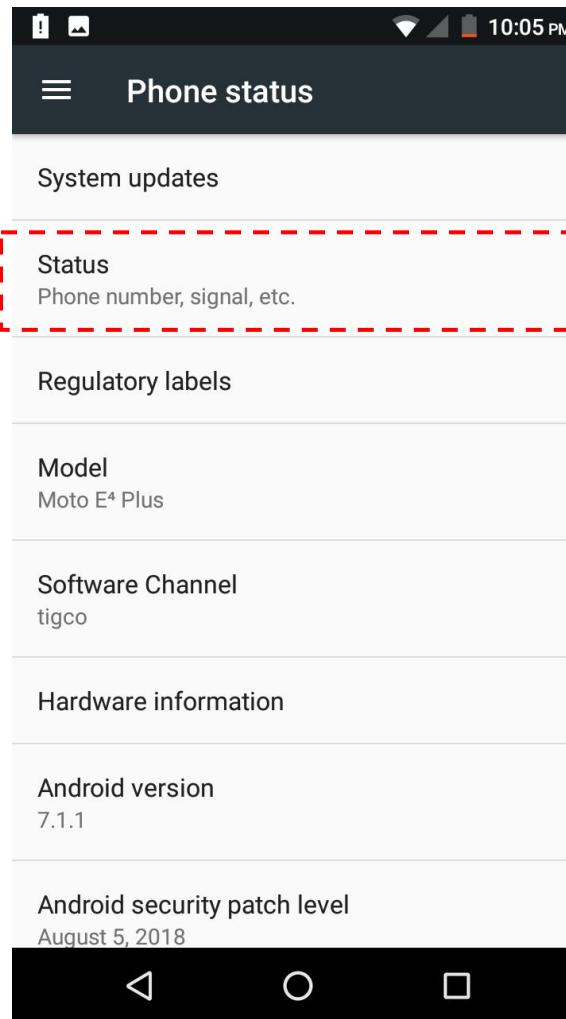
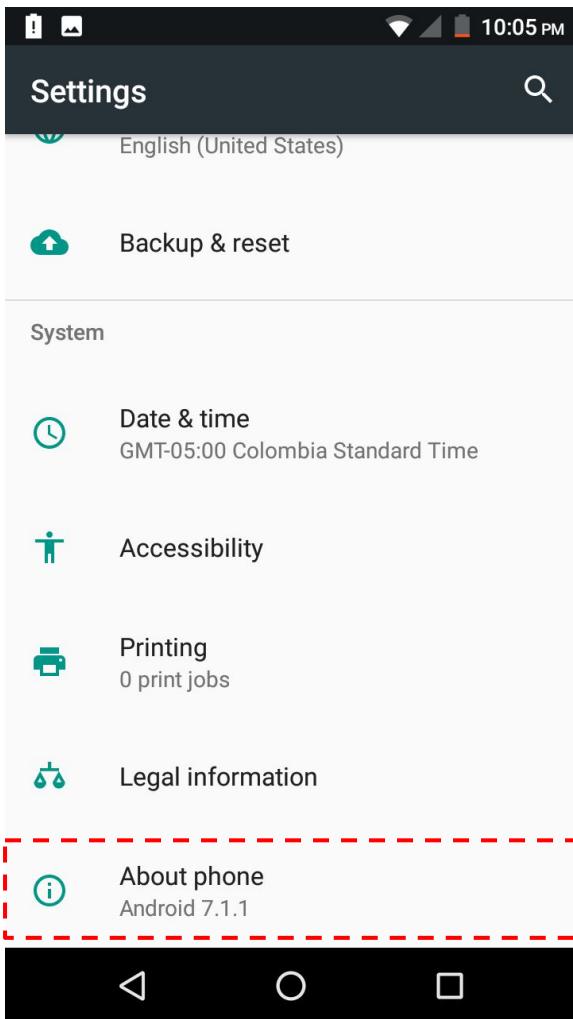
Ejecute Kismet en un laptop que tenga en casa y resuelva las siguientes preguntas mostrando la evidencia (Captura de pantalla):

- ¿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/](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?

$$\text{Rate} = \text{“Data Packet”} / \text{“Management Packet”}$$



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.

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
```

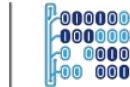
### wifi-honey Usage Example

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!