



**Desarrollo de una aplicación que permita caracterizar tramas 802.11 en redes  
inalámbricas compatible con el sistema operativo de Windows**

Otáñez Rodríguez, Esteban Francisco

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y  
Telecomunicaciones

Ing. Romero Gallardo, Carlos Gabriel

12 de marzo del 2021



## Urkund Analysis Result

Analysed Document: TESIS\_ESTEBAN\_OTANEZ\_VF.docx (D98833196)  
Submitted: 3/19/2021 1:45:00 AM  
Submitted By: cgromero@espe.edu.ec  
Significance: 2 %

### Sources included in the report:

<https://jmvinanza.wordpress.com/2015/11/05/cmo-configurar-los-canales-wifi-para-un-mejor-rendimiento-de-la-red/>).  
<https://www.tarlogic.com/programas-wifi/acrylic-wifi/#:~:text=Driver%20NDIS%253A%20Acrylic%20instala%20un,con%20Wireshark%20y%20Cain%20%2526%20Abel.Silva,>  
<https://docplayer.es/11008785-Departamento-de-electrica-y-electronica.html>

### Instances where selected sources appear:

8





## DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

### CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

#### CERTIFICACIÓN

Certifico que el trabajo de titulación, **“Desarrollo de una aplicación que permita caracterizar tramas 802.11 en redes inalámbricas compatible con el sistema operativo de Windows.”** fue realizado por el señor **Otáñez Rodríguez, Esteban Francisco**, el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 15 de marzo del 2021

Firma:



Ing. Romero Gallardo, Carlos Gabriel

C. C: 1712198066



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y  
TELECOMUNICACIONES**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**RESPONSABILIDAD DE AUTORÍA**

Yo, **Otáñez Rodríguez, Esteban Francisco**, con cédula de ciudadanía n° 1724102874 , declaro que el contenido, ideas y criterios del trabajo de titulación: **"Desarrollo de una aplicación que permita caracterizar tramas 802.11 en redes inalámbricas compatible con el sistema operativo de Windows."** es de mí autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 18 de marzo del 2021

Firma:

**Otáñez Rodríguez, Esteban Francisco**

C.C.: 1724102874



**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y  
TELECOMUNICACIONES**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**AUTORIZACIÓN DE PUBLICACIÓN**

Yo, **Otáñez Rodríguez, Esteban Francisco**, con cédula de ciudadanía n° 1724102874, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Desarrollo de una aplicación que permita caracterizar tramas 802.11 en redes inalámbricas compatible con el sistema operativo de Windows."**, en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 18 de marzo del 2021

Firma:

**Otáñez Rodríguez, Esteban Francisco**

C.C.: 1724102874

## **Dedicatoria**

Dedicado a la memoria de mi madre y abuelita

Esteban Francisco Otáñez Rodríguez

## **Agradecimientos**

Agradezco a Dios por permitirme culminar este proceso de formación en esta prestigiosa Universidad y por permitirme compartir estos momentos con mi familia.

Agradezco a mi madre y mi abuelita que desde el cielo guiaron mi camino, agradezco también por cada consejo, por todo su apoyo incondicional que recibí de ellas y por todo lo que hicieron para que pueda estudiar sin complicaciones o limitaciones.

Gracias a mis tíos, por su paciencia y su apoyo incondicional en mi formación personal y profesional.

Doy gracias también a mis hermanos que sin importar las circunstancias estuvieron conmigo con palabras de ánimo y motivándome a seguir adelante en los momentos más difíciles de mi vida.

Gracias a mi tutor el Ingeniero Carlos Romero quien me brindo su experiencia y su conocimiento para poder culminar con éxito este proyecto de titulación

Finalmente quiero agradecer a mis amigos que sin lugar a duda fueron una pieza clave durante toda mi vida universitaria.

Gracias a todos, muchas gracias.

Esteban Francisco Otáñez Rodríguez

## Índice de Contenidos

Urkund.....	2
Certificación.....	3
Responsabilidad de Autoría.....	4
Autorización de Publicación.....	5
Dedicatoria .....	6
Agradecimientos.....	7
Índice de Contenidos.....	8
Índice Tablas.....	15
Índice Figuras.....	17
Resumen.....	20
Palabras Clave .....	20
Abstract.....	21
Keywords .....	21
Capítulo I.....	22
Introducción.....	22
Antecedentes.....	22
Justificación .....	23
Objetivos.....	25
Objetivo General .....	25
Objetivos Específicos .....	25
Organización del Trabajo de Titulación .....	25



Capítulo II.....	27
Marco Teórico .....	27
Redes Wifi .....	27
Características de las Redes Wifi .....	27
Institute of Electrical and Electronics Engineers.....	27
Estandar 802.11 .....	28
Componentes Físicos de una Red Inalámbrica.....	28
Medio Aéreo.....	28
Usuarios.....	28
Dispositivos Usados en una Red Wlan .....	29
Dispositivos de Acceso al Medio.....	30
Tarjetas de Red Inalámbrica.....	30
Estación Base .....	30
Punto de Acceso .....	31
Enrutador Inalámbrico .....	31
Dispositivos de Usuario Final .....	32
Trama de Red.....	32
Tipos de Tramas .....	32
Tramas de Administración .....	33
Trama Beacon.....	33
Trama Probe Request.....	34

	10
Trama Probe Response .....	34
Trama Authentication .....	34
Trama Association Request.....	34
Trama Association Response.....	35
Tramas de Control.....	35
Trama de Enlace .....	35
Mecanismos de Protección .....	36
Privacidad Equivalente por Cable .....	37
Acceso Inalámbrico de Protección .....	37
Acceso Inalámbrico de Protección 2 .....	37
Mecanismos de Detección .....	38
Estándar 802.11 .....	39
Cabecera Mac .....	42
Sniffer .....	43
Monitoreo de Red .....	43
Analizador de Paquetes de Red Inalámbrica .....	45
Usos del Analizador de Tráfico Red.....	45
Uso Correcto .....	45
Uso Incorrecto .....	45
Analizadores de Paquetes de Redes Inalámbricas en el Mercado.....	46
Wireshark.....	46

	11
TShark.....	47
Microsoft Message Analyzer.....	47
Tcpdump .....	48
Herramientas Utilizadas .....	49
Driver Ndis Wifi.....	49
Lb Link Blwn150ah .....	50
Tarjeta de Red TL-wn722n .....	51
AirPcap Nx .....	52
Acrylic Wi-fi Professional .....	53
Tarjetas compatibles en modo monitor a travez del controlador de acrylic .....	53
Python .....	54
Scapy de Python .....	54
Función Sniff de Scapy.....	55
Base de Datos.....	55
Mysql.....	55
Capítulo III.....	57
Desarrollo del Aplicative para Caracterizar Tramas 802.11 .....	57
Diseño del Aplicative para Caracterizar Tramas 802.11 .....	57
Controladores y Modo Monitor .....	57
Herramientas de Captura .....	59
Estructura del Programa .....	60

Diseño de la Interfaz Gráfica para la Captura de Tramas y Procesamiento de Datos	60
Diagrama de Bloques del Aplicativo .....	60
Etapa de Captura .....	63
Etapa de Procesamiento .....	64
Etapa de Búsqueda y Clasificación .....	76
Control Panel.....	87
Salto Frecuencia .....	88
Canal Fijo.....	91
Compatibilidad con Python 3.....	92
Interfaz Gráfica del Aplicativo .....	93
Programa Pantalla Principal .....	93
Botón de Conexión a la Base de Datos .....	94
Base de Datos.....	95
Panel de Control Principal, de canal, ancho de banda y salto de Frecuencia.....	95
Panel de Control Principal .....	95
Control Panel de Canal, Ancho de Banda y Salto de Frecuencia .....	96
Tablas de Clasificación de las Tramas Capturadas .....	97
Detalle de Funcionamiento del Dispositivo.....	98
Capítulo IV .....	104
Captura de Tráfico de Datos y Análisis de Resultados .....	104
Pruebas de Compatibilidad con el Controlador de Acrylic.....	104

Adaptador Inalámbrico AirPcap NX.....	104
Adaptador Inalámbrico TP-LINK TL-WN722N.....	105
Adaptador Inalámbrico LB-Link BI-wn150ah .....	106
Obtención de Tráfico Wifi.....	106
Análisis de Resultados.....	107
Análisis de Datos .....	107
Protocolos de Seguridad .....	107
Canales .....	108
Eficiencia del Aplicativo.....	109
Pruebas Mediante la Captura de Tráfico Real.....	109
Tramas de Administración .....	109
Tramas de Control.....	113
Tramas de Datos.....	114
Pruebas Mediante la Inyección de Tráfico .....	116
Tramas de Administración.....	116
Tramas de Control.....	120
Capítulo V .....	124
Conclusiones y Recomendaciones.....	124
Conclusiones .....	124
Recomendaciones .....	126
Trabajos Futuros.....	127

Bibliografía .....	129
Anexos .....	133

## Índice Tablas

Tabla 1 <i>Tipo y subtipo tramas 802.11</i> .....	33
Tabla 2 <i>Tarjetas compatibles con acrylic</i> .....	53
Tabla 3 <i>Porcentaje de error las tramas Beacons</i> .....	110
Tabla 4 <i>Porcentaje de error las tramas Probe Request</i> .....	110
Tabla 5 <i>Porcentaje de error las tramas Probe Response</i> .....	110
Tabla 6 <i>Porcentaje de error las tramas Authentication</i> .....	111
Tabla 7 <i>Porcentaje de error las tramas DE authentication</i> .....	111
Tabla 8 <i>Porcentaje de error las tramas Association Request</i> .....	112
Tabla 9 <i>Porcentaje de error las tramas Association Response</i> .....	112
Tabla 10 <i>Porcentaje de error las tramas Reassociation Request</i> .....	112
Tabla 11 <i>Porcentaje de error las tramas Reassociation Response</i> .....	113
Tabla 12 <i>Porcentaje de error las tramas Acknowledgement</i> .....	113
Tabla 13 <i>Porcentaje de error las tramas Request to Send</i> .....	114
Tabla 14 <i>Porcentaje de error las tramas Clear to Send</i> .....	114
Tabla 15 <i>Porcentaje de error las tramas Data</i> .....	115
Tabla 16 <i>Porcentaje de error las tramas Beacons</i> .....	116
Tabla 17 <i>Porcentaje de error las tramas Probe Request</i> .....	117
Tabla 18 <i>Porcentaje de error las tramas Probe Response</i> .....	117
Tabla 19 <i>Porcentaje de error las tramas Authentication</i> .....	118
Tabla 20 <i>Porcentaje de error las tramas DE authentication</i> .....	118
Tabla 21 <i>Porcentaje de error las tramas Association Request</i> .....	119
Tabla 22 <i>Porcentaje de error las tramas Association Response</i> .....	119
Tabla 23 <i>Porcentaje de error las tramas Reassociation Request</i> .....	120
Tabla 24 <i>Porcentaje de error las tramas Reassociation Response</i> .....	120
Tabla 25 <i>Porcentaje de error las tramas Acknowledgement</i> .....	121

Tabla 26 *Porcentaje de error las tramas Request to Send*.....121

Tabla 27 *Porcentaje de error las tramas Clear to Send*. ....121



## Índice Figuras

Figura 1 <i>Dispositivo y conexión de una red WLAN.</i> .....	29
Figura 2 <i>Tarjeta de red inalámbrica.</i> .....	30
Figura 3 <i>Enrutador inalámbrico convencional.</i> .....	31
Figura 4 <i>Mecanismo de protección de redes WLAN.</i> .....	36
Figura 5 <i>Protocolo LAN inalámbrico 802.11.</i> .....	41
Figura 6 <i>Estructura de la cabecera Mac.</i> .....	42
Figura 7 <i>Esquema de monitoreo de red.</i> .....	44
Figura 8 <i>Interfaz del analizador de protocolos Wireshark.</i> .....	46
Figura 9 <i>Interfaz Tshark.</i> .....	47
Figura 10 <i>Interfaz del programa Microsoft Message Analyzer.</i> .....	48
Figura 11 <i>Ejecución del programa tcpdump.</i> .....	49
Figura 12 <i>Adaptador usb LB-Link BI-wn150ah.</i> .....	50
Figura 13 <i>Adaptador usb TL-wn722n.</i> .....	51
Figura 14 <i>Gestión de datos de MySql.</i> .....	55
Figura 15 <i>Canales de captura de paquetes de tarjeta Atheros.</i> .....	58
Figura 16 <i>Canales de captura de paquetes de la tarjeta Ralink.</i> .....	58
Figura 17 <i>Lista de interfaces encontradas mediante tshark.</i> .....	59
Figura 18 <i>Estructura del programa.</i> .....	60
Figura 19 <i>Diagrama de Flujo de la función Main.</i> .....	61
Figura 20 <i>Continuación de la función Main.</i> .....	62
Figura 21 <i>Continuación de la función Main.</i> .....	63
Figura 22 <i>Diagrama de flujo de la función thread_capturas.</i> .....	63
Figura 23 <i>Diagrama de flujo de la función thread_packet_handler.</i> .....	65
Figura 24 <i>Diagrama de flujo de la función packet_handler.</i> .....	66
Figura 25 <i>Diagrama de flujo de la sección de extracción de datos.</i> .....	67

Figura 26 <i>Diagrama de flujo de la sección de extracción de datos.</i> .....	67
Figura 27 <i>Ingreso de datos en la tabla de dispositivos.</i> .....	68
Figura 28 <i>Diagrama de flujo de la función de inicio, cifrado y encriptación.</i> .....	69
Figura 29 <i>Continuación de la función de inicio_cifrado_encriptacion.</i> .....	70
Figura 30 <i>Continuación de la función de inicio_cifrado_encriptacion.</i> .....	71
Figura 31 <i>Diagrama del retorno de datos de cifrado, encriptación y autenticación.</i> .....	71
Figura 32 <i>Inicio del diagrama de flujo inicio_encriptacion_cifrado.</i> .....	72
Figura 33 <i>Diagrama de flujo en caso de que exista la capa Rsn.</i> .....	73
Figura 34 <i>Diagrama de flujo en caso de que exista la capa Wpa.</i> .....	73
Figura 35 <i>Diagrama de flujo de la función cifr_to_name.</i> .....	75
Figura 36 <i>Diagrama de flujo de la función aut_to_name.</i> .....	76
Figura 37 <i>Diagrama de flujo de thread_comportamiento_aps.</i> .....	77
Figura 38 <i>Diagrama de flujo de la función búsqueda_up_ins.</i> .....	78
Figura 39 <i>Continuación del diagrama de flujo de búsqueda_up_in.</i> .....	79
Figura 40 <i>Condición C de la condicional de búsqueda_up_ins.</i> .....	80
Figura 41 <i>Diagrama de flujo de la función thread_comportamiento_dsp.</i> .....	80
Figura 42 <i>Diagrama de flujo de busqueda_up_in_dsp.</i> .....	82
Figura 43 <i>Continuación diagrama de flujo busqueda_up_disp.</i> .....	82
Figura 44 <i>Diagrama de flujo de la función thread_totales.</i> .....	83
Figura 45 <i>Diagrama de flujo Clasificaciones_totales.</i> .....	85
Figura 46 <i>Continuación de la función Clasificaciones_totales.</i> .....	86
Figura 47 <i>Condicional de la función Clasificaciones_totales.</i> .....	86
Figura 48 <i>Diagrama de flujo de la función Salto Frecuencia.</i> .....	88
Figura 49 <i>Continuación de la función Salto Frecuencia.</i> .....	88
Figura 50 <i>Solapamiento de canales en la frecuencia de 2.4 GHz.</i> .....	89
Figura 51 <i>Solapamiento de canales en la frecuencia de 5 GHz.</i> .....	90

Figura 52 Archivos para el ejecutable de control_c.....	92
Figura 53 Archivos disponibles en control_c.....	92
Figura 54 Pantalla principal. ....	94
Figura 55 Botón de conexión con la base de datos. ....	94
Figura 56 Base de datos Windows Sniffer. ....	95
Figura 57 Panel de control de la interfaz. ....	96
Figura 58 Control panel de la tarjeta.....	97
Figura 59 Tablas de clasificación de las tramas capturadas. ....	98
Figura 60 Ventana principal sin conexión a la base de datos. ....	98
Figura 61 Activación del panel de control principal para la selección de la interfaz. ....	99
Figura 62 Despliegue de los adaptadores de red. ....	99
Figura 63 Selección de la tarjeta de red y activación del Control Panel. ....	100
Figura 64 Sección de Características por ap. ....	101
Figura 65 Sección Contador de tramas ap. ....	101
Figura 66 Contador de tramas por dispositivos.....	102
Figura 67 Sección Contador de trama totales.....	103
Figura 68 Captura del trafico 802.11 mediante la tarjeta AirPcap NX. ....	105
Figura 69 Captura del trafico 802.11 mediante la tarjeta Tp-Link Tl-Wn722n.....	105
Figura 70 Captura del trafico 802.11 mediante la tarjeta Lb-Link Bl-em150ah. ....	106
Figura 71 Protocolos de seguridad escaneados. ....	108
Figura 72 Usuarios conectados a los diferentes canales. ....	108
Figura 73 Porcentaje total de pérdidas en las tramas capturadas.....	115
Figura 74 Porcentaje total de pérdidas en las tramas capturadas con la inyección.....	122
Figura 75 Direcciones Mac de los dispositivos vinculados a sus respectivos Ap. ....	123

## **Resumen**

En las últimas décadas con el avance tecnológico y la necesidad de comunicarse para intercambiar información ha generado que las personas recurran al uso masivo de redes inalámbricas tanto a nivel empresarial, así como en sus hogares; éste incremento en el uso de redes inalámbricas ha provocado que sean más susceptibles a ataques y que estos sean perjudiciales para el desempeño de la red, así como para la seguridad de la información de los usuarios. El presente proyecto se desarrolla un aplicativo compatible con el sistema operativo Windows que permite caracterizar y mostrar las tramas 802.11 de una red inalámbrica en tiempo real, de manera sencilla y automatizada. Para poder realizar la captura de tráfico se utilizaron los chipsets compatibles con Windows y con el controlador de Acrylic, el cual permite colocar la tarjeta de red en modo monitor al igual que módulos AirPcap NX tanto en mono canal como multicanal y así obtener información sobre los protocolos inalámbricos. La implementación del algoritmo utiliza la técnica de sniffing que permite en modo de ataque pasivo capturar el tráfico generado en conexiones locales, así como el tráfico generado por las conexiones de los otros usuarios. Los resultados obtenidos mediante la captura del tráfico proporcionan tramas de administración, datos, control y direcciones MAC/IP; mismos que serán analizados para comprobar la eficiencia del aplicativo desarrollado, comparando sus resultados con otro software llamado Wireshark y de este modo exponer conclusiones sobre su uso, desempeño y eficiencia.

### **Palabras Clave**

- **TRAMA 802.11**
- **SNIFFER**
- **WIRESHARK**
- **ANALIZADOR DE TRÁFICO**

### **Abstract**

In recent decades, with technological advancement and need to communicate to exchange information, people have resorted to the massive use of wireless networks both at the business level, as well as at home; This increase of the wireless networks has made them more susceptible to attacks and that these are detrimental to the performance of the network, as well as to the security of users' information. This project develops an application compatible with the Windows operating system that allows characterizing and displaying 802.11 frames of a wireless network in real time, in a simple and automated way. In order to capture the traffic, chipsets compatible with Windows and with the Acrylic driver were used, which allows the network card to be placed in monitor mode as well as AirPcap NX modules in both single and multi-channel channels and thus obtain information about the wireless protocols. The implementation of the algorithm uses the sniffing technique that allows, in passive attack mode, to capture the traffic generated in local connections, as well as the traffic generated by the connections of other users. The results obtained by capturing the traffic provide management frames, data, control and MAC/IP addresses. They will be analyzed to check the efficiency of the application developed, comparing its results with other software called Wireshark and thus present conclusions about its use, performance and efficiency.

### **Keywords**

- **FRAME 802.11**
- **SNIFFER**
- **WIRESHARK**
- **TRAFFIC ANALYZER**

## Capítulo I

### Introducción

#### Antecedentes

Para el desarrollo del Proyecto se han tomado en consideración trabajos de investigación del repositorio digital de la Universidad de las Fuerzas Armadas ESPE y otras instituciones a nivel nacional.

Como primer antecedente tenemos el trabajo desarrollado en la Universidad de las Fuerzas Armadas ESPE, el cual tiene como tema y objetivo principal el “Desarrollo de un aplicativo para caracterizar tramas 802.11 en redes inalámbricas utilizando software libre” (Lara, 2020), del cual se concluyó que la información de las tramas 802.11 dan a conocer, por medio de la cabecera MAC la información de la misma como el tipo, subtipo, MAC address, su encriptación etc., así como la cantidad de bytes que ocupa cada una de las tramas, el conocimiento de esta información es crucial para el desarrollo del aplicativo.

Dentro de la investigación realizada en la Universidad Técnica de Ambato, la cual lleva como tema “Las Redes Inalámbricas y su Incidencia en la Interconexión de las Redes Industriales en los Laboratorios de la Carrera de Ingeniería Industrial en Procesos de Automatización de la Facultad de Ingeniería en Sistemas Electrónica e Industrial” (Morales & Córdova, 2010), cuyo objetivo principal fue “Determinar la incidencia de las Redes inalámbricas en el mejoramiento de la interconexión de las redes industriales en los laboratorios de la carrera de ingeniería industrial en procesos de automatización de la FISEI” y que concluyo que en el laboratorio se requiere la implementación de un sistema de interconexión entre los laboratorios de la carrera de ingeniería industrial en procesos de automatización para poder comunicar las células de trabajo existentes y formar un campo de experimentación para los estudiantes.

En otro trabajo de la misma Universidad Técnica de Ambato que lleva como tema “Red Inalámbrica tipo malla (WNM) estándar 802.11 de transmisión y la optimización de cobertura en los Colegios de la Provincia de Tungurahua” (Manzano & Vásquez, 2014), el cual tuvo como objetivo general “Determinar como la estructura de la red inalámbrica incide en la optimización de la cobertura para mejorar la transmisión de datos” y concluyo en que el acceso a la red de datos de la Unidad Educativa Mayor Ambato es lenta ya que existe varias redes inalámbricas las cuales no pueden brindar la cobertura ni seguridad necesaria en la transmisión de datos.

Como último antecedente tenemos el trabajo investigativo realizado en la Escuela Superior Politécnica de Chimborazo que tiene como tema y objetivo el “Estudio del rendimiento del estándar 802.11n en la comparación con dispositivos con el estándar 802.11b/g en la transmisión de datos” (Loayza, 2010), este trabajo concluyo que el estándar 802.11n es el estándar que mejor transmite datos, texto, audio y video.

### **Justificación**

Las redes inalámbricas a diferencia de las redes cableadas permiten transmitir información a través de un medio de propagación no físico, permitiendo un gran alcance y una gran cantidad de dispositivos conectados, evitando tener una conexión física y proporcionando que los dispositivos tengan un alto grado de movilidad. En las redes inalámbricas debido a que la información está disponible para todos usuarios que se encuentren dentro de la red y que la información viaja a través de un medio no físico (el aire) convierte a esta tecnología vulnerable, por lo que se requieren de protocolos y mecanismos que garanticen la seguridad de la información.

Un aspecto de suma importancia para la seguridad en redes inalámbricas son las técnicas y herramientas para el análisis de tráfico, debido a que permiten la detección de ataques, así como el control de usuarios; además de la monitorización de la red que permite conocer el estado de seguridad de esta. El proceso de monitoreo de

redes y servicios es de suma importancia para cualquier organización, ya que de esto depende conocer el comportamiento general de su infraestructura de comunicaciones.

La falta de conocimiento sobre protocolos de red para interpretar los datos obtenidos mediante software que permiten analizar el tráfico compatible con el sistema operativo de Windows ha desencadenado que toda la información capturada sea difícil de manejar puesto que algunas herramientas utilizan líneas de comando y es necesaria la configuración del software. Además, debido a la gran cantidad de datos que capturan imposibilita su óptimo desempeño en tiempo real por lo que no siempre se encuentran en funcionamiento y esto no permite una generación de informes de la situación actual y real en la que se encuentra la red (Gonzalez, 2014).

Existen varias herramientas que en la actualidad son compatibles con el sistema operativo de Windows y permiten realizar el análisis de tramas del estándar 802.11 tales como Wireshark, Microsoft Message Analyzer, Windump, PRTG Network Monitor, entre otros; estas herramientas presentan limitaciones en su funcionamiento en tiempo real (licencia gratuita), así como requerimientos de modificación de drivers y controladores que no se permite realizar dentro del sistema operativo de Windows, y si se desea mejorar el rendimiento e incrementar las funcionalidades de estas herramientas se debe realizar la compra de costosas licencias o pagos a los propietarios. Es por ello que se plantea el desarrollo de un aplicativo compatible con el sistema operativo de Windows que permita caracterizar las tramas 802.11 en redes inalámbricas, con una interfaz amigable con el usuario y que le permita entender cómo están comportándose las tramas en tiempo real, sin necesidad de tener mucho conocimiento en análisis de redes (Gonzalez, 2014).



## **Objetivos**

### ***Objetivo General***

Desarrollar una aplicación que permita caracterizar tramas 802.11 en redes inalámbricas compatible con el sistema operativo de Windows.

### ***Objetivos Específicos***

- Fundamentar científicamente la caracterización de tráfico de redes y herramientas de software libre compatibles con Windows para la captura del tráfico.
- Analizar el tráfico de redes inalámbricas para escoger las características y parámetros requeridos en el proyecto de investigación.
- Diseñar una aplicación que permita caracterizar tramas 802.11 en redes inalámbricas compatible con el sistema operativo de Windows.
- Realizar pruebas de funcionamiento de la aplicación en casos reales.

## **Organización del Trabajo de Titulación**

El presente trabajo está organizado de la siguiente forma:

El capítulo I se mencionan los antecedentes, justificación, y los objetivos del trabajo de titulación, el capítulo II habla sobre el fundamento teórico, enfocándose en las redes wifi, tramas de red, tipos de trama de red, definición de un sniffer y el tipo de tarjeta con el cual se van a realizar la captura de las tramas, en el capítulo III se presenta mediante diagramas de flujo cómo funciona el algoritmo desarrollado en Python, así como también la interfaz gráfica y las tablas de datos con la información procesada para que el usuario pueda visualizarla, en el capítulo IV se realiza un análisis de las pruebas obtenida mediante tráfico de red 802.11 real y simulado, analizando el porcentaje de error de pérdida en la captura de paquetes, el capítulo V se detallan las

conclusiones, recomendaciones y trabajos futuros que pueden desarrollarse a partir de este trabajo de titulación.

## Capítulo II

### Marco Teórico

#### Redes Wifi

WI-FI se utiliza para cualquier tipo de red instalada, se basa en implementar uno o más puntos de acceso en un lugar determinado; tomando esto en consideración, esta tecnología se suele utilizar principalmente para redes de área local (Carballar & Carballar Falcón, 2010).

De manera comercial se puede encontrar dos tipos de redes locales en uso: las de tipo alámbrica que se denotan con el uso de cables y las de tipo inalámbrico o redes WI-FI. Las dos tipos de redes hacen exactamente lo mismo: La interconexión de ordenadores, equipos y otro tipo de dispositivos informáticos para poder compartir recursos entre sí (Carballar & Carballar Falcón, 2010).

#### Características de las Redes Wifi

Una de las principales características de este tipo de redes es reducir el uso de la instalación cableada haciéndola más sencilla, además, se puede conectar en áreas difíciles de implementar una conexión cableada, y de manera comercial son muy accesibles; también se recalca que se pueden conectar equipos sin tener que invertir en infraestructura adicional en la nueva red, la Wifi Alliance certifica que todos aquellos dispositivos que implementen WI-FI sean compatibles en su totalidad alrededor del mundo (Carballar & Carballar Falcón, 2010).

#### Institute of Electrical and Electronics Engineers

Conocido también por sus siglas IEE, el Instituto de Ingenieros Eléctricos y Electrónicos, es una asociación de profesionales que se dedica a la estandarización y demás actividades académicas a nivel mundial. Es la mayor asociación a nivel internacional sin fines de lucro orientada a las nuevas tecnologías y con profesionales,

como ingenieros en eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación (Andreu, Pellejero, & Lesta, 2006).

### **Estandar 802.11**

Estándar que fue ratificado en julio de 1997 por parte de la IEEE. Funciona en la banda de 2.4GHz con velocidad de transmisión máxima de 2Mbps. Incluye velocidad de transmisión de 1Mbps y 2Mbps, dependiendo de la distancia entre el punto de acceso y la estación inalámbrica y de las condiciones de utilización del canal. Utiliza las modulaciones FHSS y DSSS en la capa de enlace y DBPSK, DQPSK Y GFSK en la capa física (Andreu, Pellejero, & Lesta, 2006).

### **Componentes Físicos de una Red Inalámbrica**

Dentro de los componentes físicos de una red inalámbrica podemos mencionar los siguientes:

#### ***Medio Aéreo***

Un primer elemento que a pesar de ser intangible, debe ser considerado al implementar WLANs, el medio aéreo ya que es el medio para la propagación de las señales inalámbricas. El aire es el “conducto” a través del cual los datos fluyen entre los dispositivos finales y la infraestructura de red. Similar al comportamiento en las comunicaciones convencionales, a medida que los dispositivos están más distantes es difícil mantener la comunicación y conexiones, especialmente en ambientes de alto ruido e interferencia (Jiménez, 2015).

#### ***Usuarios***

Un usuario puede ser cualquier ente que hace uso de la red inalámbrica. Uno de los tipos de usuario más comunes es una persona cualquiera, como por ejemplo un empresario que accede a Internet desde una WLAN pública, o un analista de crédito que consulta una aplicación de cartera en la WLAN corporativa. Otro tipo de usuario

puede ser un robot que recibe instrucciones (mediante la WLAN) por parte de un servidor que controla un proceso automatizado de manufactura; o una cámara de vigilancia que es controlada en forma inalámbrica desde una ubicación remota en cualquier lugar (Jiménez, 2015).

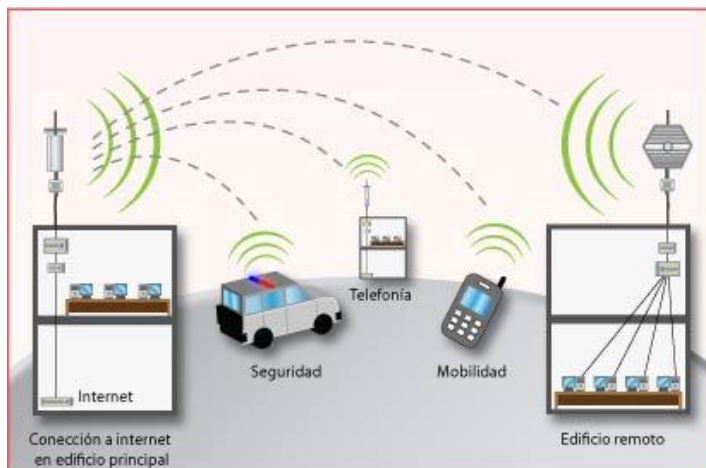
### Dispositivos Usados en una Red Wlan

Las redes inalámbricas utilizan componentes de iguales características a las redes LANs cableadas. Estos comprenden dos diferentes clases de dispositivos:

- Dispositivos de acceso al medio como tarjetas de red inalámbricas y estaciones base (puntos de acceso, enrutadores inalámbricos).
- Dispositivos de usuario final como computadores, portátiles, agendas digitales, cámaras de video, impresoras, etc. (Jiménez, 2015), como se muestra en la Figura 1.

### Figura 1

*Dispositivo y conexión de una red WLAN.*



*Nota.* Tomado de *UF1875 - Gestión de recursos, servicios y de la red de comunicaciones*, por Toro J., 2015, Universidad Autónoma de Puebla, Editorial Elearning, S.L.

## Dispositivos de Acceso al Medio

Para el acceso a una red WLAN se requiere una infraestructura tecnológica adecuada que facilite la conexión a la red e intercambiar datos. Esto se obtiene usando elementos como tarjetas de red y dispositivos que trabajan como estaciones base, puntos de acceso y enrutadores inalámbricos (Jiménez, 2015).

### ***Tarjetas de Red Inalámbrica***

La tarjeta de red inalámbrica también conocida como NIC (Network Interface Card) provee la interface y el radio que comunica el dispositivo de usuario final con la infraestructura de red WLAN. La hay en varias configuraciones, y es así como algunas NIC inalámbricas van en el interior de los dispositivos como computadores de escritorio o portátiles y otras se conectan exteriormente a través de puertos USB o ranuras PCMCIA (Jiménez, 2015). La Figura 2 muestra el aspecto físico de una tarjeta de red inalámbrica (Intercompras, 2015).

### **Figura 2**

*Tarjeta de red inalámbrica.*



*Nota.* Tomado de *TP-LINK\_TL-WN751ND*, por Intercompras., 2015, Intercompras (<https://n9.cl/8cpzg>).

### ***Estación Base***

Una estación base es una instalación fija de radio para la comunicación media, baja o alta intensidad de modo bidireccional. Se usa para comunicar con una o más

radios móviles o teléfonos celulares. Las estaciones base usualmente se usan para interconectar radios de baja potencia, como por ejemplo la de un teléfono móvil, un teléfono inalámbrico o un portátil con una tarjeta Wifi (Jiménez, 2015).

### ***Punto de Acceso***

Es un equipo que asume la función de repetidor de señales y permite la conectividad de los dispositivos inalámbricos. Este elemento opera de manera similar a la de un concentrado cableado (hub) y maneja un ancho de banda por equipo que baje en la medida en que más dispositivos se comuniquen (Jiménez, 2015).

### ***Enrutador Inalámbrico***

Son dispositivos utilizados en hogares y oficinas para conectarse a una red Internet o a una red corporativa. Además de comportarse como puntos de acceso (con funciones de concentración, amplificación y repetición) son dispositivos más inteligentes que tienen la función primaria de permitir que los equipos cableados e inalámbricos en una red accedan a una distinta red (Jiménez, 2015).

La Figura 3 muestra el aspecto de un enrutador inalámbrico convencional (PC Tecnología, 2017).

### **Figura 3**

*Enrutador inalámbrico convencional.*



*Nota.* Tomado de Tp Link Router Inalámbrico, por PC Tecnología., 2015, PC Tecnología (<https://n9.cl/712kd>).

### ***Dispositivos de Usuario Final***

También se denominan dispositivos cliente y son los elementos más visibles de una red inalámbrica. Suministran la plataforma física para que las aplicaciones inalámbricas provean servicios de red como captura y despliegue de datos, procesamiento de información, detección de ubicación y además comunicaciones de voz. Estos dispositivos pueden ser transportados por los usuarios finales o ubicados en sitios determinados dentro de las instalaciones de la organización (Jiménez, 2015).

### **Trama de Red**

Una trama en redes es una unidad para el envío de datos. Es una serie sucesiva de bits, organizada y transportada de forma cíclica, la cual permiten en la recepción tomar esta información. Es el equivalente de paquete de datos, en el nivel de red del modelo OSI (Oliva, 2013).

Para delimitar una trama se pueden emplear cuatro métodos, el tracker:

- Por conteo de caracteres.
- Por secuencia de bits.
- Por violación de nivel básico (Oliva, 2013).

### **Tipos de Tramas**

Las tramas pueden ser clasificadas dada la función que realizan, en el estándar 802.11 se tiene 3 tipos de tramas en específico y estas son:

- Tramas de datos: realiza la operación de transportar datos o información dirigidos hacia las capas superiores.
- Tramas de control: se encarga del control de acceso al medio, entregando tramas de datos hacia las distintas estaciones.



- Tramas de gestión o administración: mantiene la comunicación entre estaciones, transportando de esta manera la información de gestión, exceptuando las capas superiores (Páez, 2015).

En la Tabla 1 se muestran los tipos y subtipos de tramas del estándar 802.11.

**Tabla 1**

*Tipo y subtipo tramas 802.11.*

<b>Trama</b>	<b>Tipo</b>	<b>Subtipo</b>
Association Response	0	1
Reassociation Request	0	2
Reassociation Response	0	3
Probe Request	0	4
Probe Response	0	5
Association Request	0	7
Beacon	0	8
Authentication	0	11
RTS	1	11
CTS	1	12
ACK	1	13

### **Tramas de Administración**

#### ***Trama Beacon***

El objetivo de esta trama es informar a las estaciones más cercanas cuando aparezca alguna red wifi, todo esto enviando el AP de manera constante y con sus respectivas características para conectarse, de igual manera hace una lista de los AP que están disponibles en todos los canales 802.11 (Páez, 2015).

### ***Trama Probe Request***

Esta trama es enviada por aquellos clientes que requieren información de un punto de acceso, con la condición de que estos se encuentre en el rango de cobertura y con el objetivo de especificar su SSID en broadcast (Páez, 2015).

### ***Trama Probe Response***

Esta trama es la respuesta dada por la estación al momento de recibir un Probe Request, esta solo la recibe aquel cliente que realizó dicho pedido (unicast) (Páez, 2015).

### ***Trama Authentication***

El cliente procede enviar una trama de autenticación donde envía el AP, con el fin de verificar su identidad y así este pueda unirse a la red, para realizar esta operación, se pueden encontrar dos tipos de autenticación:

**Autenticación Abierta.** El cliente procede a enviar una trama de autenticación y el punto de acceso envía una trama como respuesta de autenticación donde indica si la estación lo acepta o no (Páez, 2015).

**Autenticación con Clave Compartida.** En este tipo de autenticación la estación conoce la clave con la que se accede a la red. El punto de acceso procede a comprobar si dicha estación conoce o no la llave, enviando una respuesta en forma de trama de texto, la estación una vez validada su identidad procederá a enviar la llave encriptada y una trama aceptando a la estación (Páez, 2015).

### ***Trama Association Request***

Esta trama es usada por una estación cliente con la cual se empieza el proceso de asociación que hará que el punto de acceso reserve recursos y se pueda sincronizar, estableciendo un ID de asociación con la estación (Páez, 2015).

### ***Trama Association Response***

El punto de acceso envía esta trama como respuesta a una Association Request, para informar si se acepta o rechaza a la estación que solicita el pedido (Páez, 2015).

### ***Tramas de Control***

**Trama Request To Send (RTS).** Se empieza la comunicación con el envío de una RTS de dos vías para poder enviar tramas, tratar de que las colisiones sean mínimas, siempre y cuando dos estaciones se asocien al mismo AP (Páez, 2015).

**Trama Clear To Send (CTS).** Esta trama informa que el canal está libre de transmisiones dada la trama RTS que empezó la comunicación, estas ayudan a controlar las colisiones existentes al poseer los datos del valor de tiempo, dada esta trama, si la estación solicitante transmite las demás no lo pueden hacer (Páez, 2015).

**Trama Acknowledgement (ACK).** Esta trama asegura que las demás puedan acceder, al no encontrarse ningún error el cliente receptor envía una ACK al emisor, por otro lado, si el cliente emisor no acoge una ACK este se envía de nuevo (Páez, 2015).

### ***Trama de Enlace***

El objetivo de la capa de enlace es hacer que la información fluya libre de errores, entre dos dispositivos o máquinas que estén conectadas de forma directa (servicio orientado a la conexión). Para lograr esto se tiene que montar bloques de información (tramas en esta capa), otorgarles una dirección de capa de enlace (Dirección MAC), gestionar la detección o corrección de errores, y encargarse del “control de flujo” entre equipos (evitando que un equipo más rápido desborde a uno más lento) (Oliva, 2013).

Cuando el medio está compartido entre más de dos equipos es necesario regular el uso del mismo. Esta tarea se realiza en específico en la subcapa de control de acceso al medio (Oliva, 2013).

Dentro del grupo de normas IEEE 802, la subcapa de enlace lógico se recoge en la norma IEEE 802.2 y está adaptada para todos tipos de redes (Ethernet o IEEE 802.3, IEEE 802.11 o Wifi, IEEE 802.16 o WiMAX, etc.); todas detallan una subcapa de acceso al medio, así como una capa física de distinta característica (Oliva, 2013).

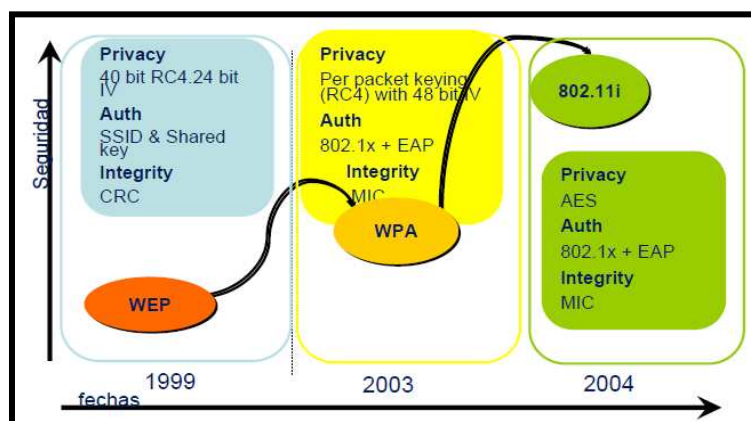
### Mecanismos de Protección

Las redes WLAN poseen muchos problemas de seguridad que se dan a consecuencia del medio de transmisión, el aire, cuya facilidad de acceso es atractivo para cualquier atacante dispuesto a realizar una intrusión. La encriptación es uno de los métodos más utilizados y por el cual se puede proteger la información enviada. En la actualidad se utilizan WEP, WPA y WPA2 (Oliva, 2013).

Los mecanismos de protección de las redes WLAN se muestran en la Figura 4.

**Figura 4**

*Mecanismo de protección de redes WLAN.*



*Nota.* Tomado de *Redes de comunicaciones industriales*, por Alonso O., 2013, Editorial UNED.

### **Privacidad Equivalente por Cable**

También denominado WEP por sus siglas en inglés (Wired Equivalent Privacy). Las contraseñas WEP pueden ser vulneradas por medio de un aircrack-ng, poseen una vida útil corta, es utilizada para el cifrado y para la autenticación en el protocolo 802.1x.

### **Acceso Inalámbrico de Protección**

También denominado WAP por sus siglas en inglés (Wireless Application Protocol). Se puede encontrar a este tipo de acceso en dos presentaciones: 802.1X (Enterprise) la cual usa EAP (Protocolo de autenticación extensible) y PSK que utiliza una clave entre el punto de acceso y el radio del cliente, por otra parte WPA utiliza TKIP (Protocolo de integridad de clave temporal) en modo de encriptación (Stanfanick, 2018).

Este ID esta denotado por 0x221 coincidiendo con el ID del proveedor, dado esto primero la estación comprueba la OUI (Identificador Único de la Organización) para después identificar si esta información encriptada pertenece a WPA, por lo que deberá estar en 00-50-f2 (Holla, 2017).

### **Acceso Inalámbrico de Protección 2**

También denominado WAP2. El acceso protegido Wi-Fi 2 se realizó principalmente como una actualización de los protocolos de seguridad anteriores, es decir, WEP y WPA. El estándar WPA2 incluía todos los requisitos de seguridad en línea con los estándares de seguridad de IEEE 802.11i. Esta actualización ofrece un control de acceso a la red más seguro y una mayor protección de los datos. Tras la aprobación de la especificación IEEE 802.11i en julio de 2004, se publicó el WPA2 basado en el mecanismo Robust Security Network (RSN) (Stanfanick, 2018).

El WPA2 soporta los mecanismos disponibles en el WPA junto con algunas actualizaciones que se enumeran a continuación:

- Mayor apoyo tanto a la infraestructura como a las redes ad hoc en cifrado y autenticación. El anterior protocolo de seguridad (WPA) se limitaba únicamente a las redes de infraestructura.
- Provisión de caché de claves que pretendan acceder. Con ello se pretende principalmente reducir los costos de itinerancia entre los puntos de acceso.

### **Mecanismos de Detección**

- **Tripwire:** ejecuta varios checksums sobre ficheros de configuración para posteriormente compararlos con una base de datos para así aceptar solo los valores considerados como buenos o correctos.
- **Snort:** realiza el monitoreo del distinto tráfico que pueden generar intrusos o diferentes tipos de ataques o atacantes; esto ayuda a auditar un sistema o tener un control sobre el mismo. El fin de este monitoreo no es proteger a la red frente a ataques que puedan darse sino dar información sobre su ocurrencia.
- **IDS:** es una herramienta que realiza un monitoreo de eventos en busca de intentos de intrusión o ataque. Un IDS detecta actividades anormales escuchando el tráfico de información con el objetivo de captar un intento de intrusión.
- **WIDS:** este sistema de protección compara las direcciones MAC que va encontrando con aquellos dispositivos Wifi con autorización que se tengan registrados. Al existir los métodos de suplantación de direcciones MAC esta herramienta también revisa la fiabilidad de la firma digital del producto (Oliva, 2013).

### **Estándar 802.11**

El estándar IEEE 802.11 define varios tipos de tramas cada de las cuales tiene un objeto en concreto. Se procede a anunciar los puntos de acceso, asociar estaciones existentes, autenticar, etc. Estas funciones se gestionan mediante tramas especiales, que se diferencian de las tramas ya existentes propias de la transmisión. Se pueden clasificar distintas tramas según su función y desempeño (Íñigo & Barceló, 2009).

Se tienen distintas tramas, entre las cuales existen: tramas de datos, las de transporte de información a capas superiores, tramas de gestión para mantener las comunicaciones y tramas de control que como su nombre lo indica, proceden a controlar el medio (Íñigo & Barceló, 2009).

De forma general, el estándar IEEE 802.11 se denomina “Wi-Fi”. Es un sistema de contienda que utiliza un proceso CSMA/CA de acceso al medio. CSMA/CA especifica un procedimiento de postergación de manera aleatoria para todos los nodos que están esperando poder transmitir. La oportunidad más probable para la contención de medio es el momento en que esté disponible. Hacer el back off de los nodos para un período aleatorio reduce la probabilidad de colisión en gran medida (Íñigo & Barceló, 2009).

Las redes 802.11 utilizan acuses de recibo para confirmar que la trama enviada se recibió de manera correcta. Si la estación transmisora no puede detectar la trama de reconocimiento enviada, ya sea porque la trama de datos original o el reconocimiento no las recibieron intactos, se retransmite la trama nuevamente. Este reconocimiento explícito supera la interferencia y otros problemas relacionados con la estación (Íñigo & Barceló, 2009).

Otros servicios admitidos por la 802.11 son la autenticación, asociación (conexión a un dispositivo inalámbrico) y privacidad (encriptación). A continuación, se describen los campos que incluyen la trama 802.11:

- **Campo Versión de Protocolo:** la versión de la trama 802.11 en uso.
- **Campos Tipo y Subtipo:** identifican una de las tres funciones y subfunciones de la trama (control, datos y administración).
- **Campo A DS:** se establece en 1 para las tramas de datos destinadas al sistema de distribución (dispositivos en la estructura inalámbrica).
- **Campo Desde DS:** se establece en 1 para las tramas de datos que salen del sistema de distribución.
- **Campo más Fragmentos:** se establece en 1 para las tramas que tienen otro fragmento.
- **Campo Reintentar:** se establece en 1 si la trama es una retransmisión de una trama anterior.
- **Campo Administración de Energía:** se establece en 1 para indicar que un nodo estará en el modo de ahorro de energía.
- **Campo más Datos:** se establece en 1 para indicarle a un nodo en el modo de ahorro de energía que se almacenan más tramas en búfer para ese nodo.
- **Campo Privacidad Equivalente por Cable (WEP):** Se la pone en 1 si la trama contiene información encriptada mediante WEP para seguridad.
- **Campo Orden:** Se la pone en 1 en una trama de tipo de datos que utiliza la clase de servicio estrictamente ordenada (no requiere reordenamiento).
- **Campo Duración/ID:** según el tipo de trama, representa el tiempo que se requiere en microsegundos para transmitir la trama o una identidad de asociación (AID) para la estación que transmitió dicha trama.
- **Campo Dirección de Destino (DA):** contiene la dirección MAC del nodo de destino final en la red.

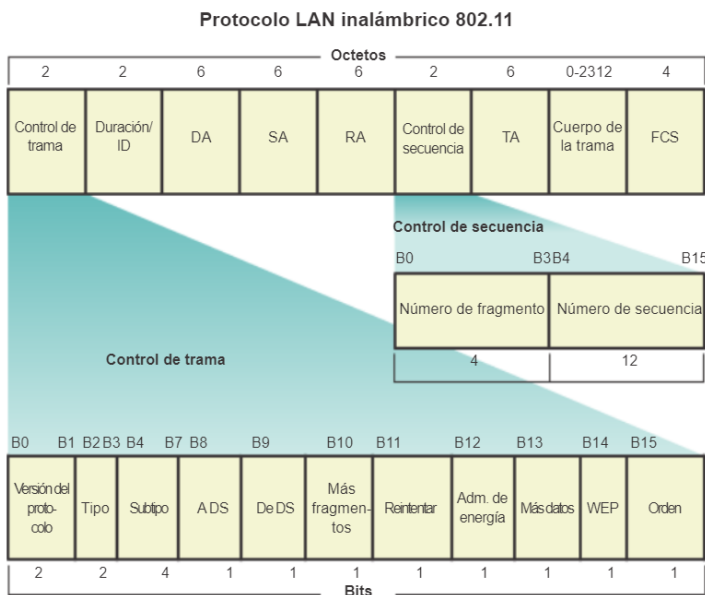


- **Campo Dirección de Origen (SA):** contiene la dirección MAC del nodo que inició la trama.
- **Campo Dirección del Receptor (RA):** contiene la dirección MAC que identifica al dispositivo inalámbrico que es el destinatario inmediato de la trama.
- **Campo Número de Fragmento:** indica el número de cada fragmento de la trama.
- **Campo Número de Secuencia:** indica el número de secuencia designada a la trama. Las tramas retransmitidas se identifican con números de secuencia que están duplicados.
- **Campo Dirección del Transmisor (TA):** contiene la dirección MAC que identifica al dispositivo inalámbrico que procedió a transmitir la trama.
- **Campo Cuerpo de la Trama:** contiene la información que se transporta. En las tramas de datos; generalmente se trata de un paquete IP.
- **Campo FCS:** contiene una comprobación de redundancia cíclica (CRC) de 32 bits de la trama (Íñigo & Barceló, 2009).

La Figura 5 muestra las partes de la trama correspondientes al protocolo 802.11 (Itesa, 2017).

### **Figura 5**

*Protocolo LAN inalámbrico 802.11.*



*Nota.* Tomado de *Control de Acceso al Medio*, por Itesa., 2017, Itesa (<https://n9.cl/z8si>).

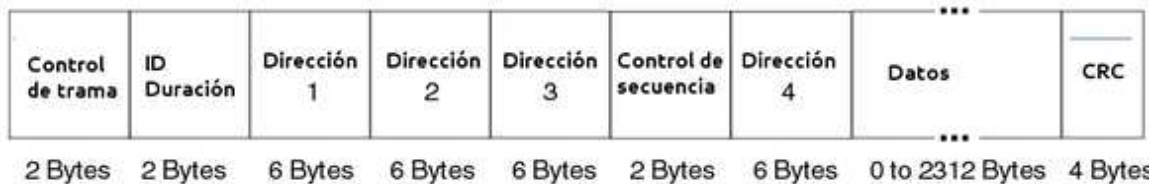
### **Cabecera Mac**

En informática y telecomunicaciones, el control de acceso al medio MAC (Media Access Control) es el conjunto de mecanismos y protocolos de comunicaciones a través de los cuales varios "interlocutores" (dispositivos en una red, como computadoras, teléfonos móviles, etcétera) se ponen de acuerdo para compartir un medio de transmisión común (por lo general, un cable eléctrico o fibra óptica, o en comunicaciones inalámbricas el rango de frecuencias asignado a su sistema) (Enriquez, Hamilton, & Taha Ahmed, 2014).

La cabecera MAC, cuya estructura se muestra en la Figura 6 a continuación, está formada por varios campos de longitud fija (Wikimedia, 2020).

### **Figura 6**

*Estructura de la cabecera Mac.*



*Nota.* Tomado de *Trama 802.11*, por Wikimedia., 2020, Wikimedia ([https://upload.wikimedia.org/wikipedia/commons/thumb/9/93/Trama\\_802.11.png/600px-Trama\\_802.11.png](https://upload.wikimedia.org/wikipedia/commons/thumb/9/93/Trama_802.11.png/600px-Trama_802.11.png)).

### Sniffer

Un Sniffer es un pequeño programa que captura cualquier flujo de información que pase por el ordenador en el que se ejecuta. Esta información no tiene por qué obtenerse de modo normal, sino que los sniffers leen esta información, aunque no tenga por destino este ordenador. Tras capturar la información pueden interpretarla y guardarla para usos futuros (Mouteira, 2004).

Aparentemente el uso de los sniffers estaría limitado a topologías en forma de bus, ya que es este el medio tradicional para la difusión punto a multipunto. Hay que tener en cuenta que para que no puedan funcionar los sniffers no es suficiente con que la topología física este estructurada en estrella, sino también la topología lógica, ya que muchas de las redes con este formato tienen una lógica en bus o anillo, permitiendo que los monitores de red actúen con libertad (Mouteira, 2004).

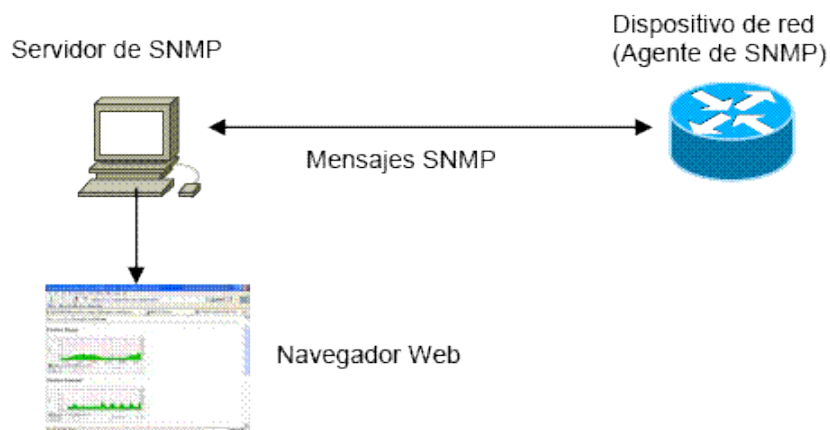
### Monitoreo de Red

El buen servicio de usuario comprende de monitorear las actividades de los dispositivos conectados en la red para detectar las fallas que puedan existir y poder corregirlas. Un esquema que pueda notificar las fallas en la red es fundamental ya que nos ayuda a mostrar su comportamiento mediante un análisis y recolección de tráfico (Menéndez, 2016).

La siguiente Figura 7 muestra un esquema de monitoreo de red (Junco, 2012).

**Figura 7**

*Esquema de monitoreo de red.*



*Nota.* Tomado de *Los recursos de red y su monitoreo*, por Junco G., 2012, Monografías (<https://n9.cl/pkpl>).

Hablar de sistemas de monitoreo de servicios de red en si sistemas operativos de red o desktop resultaba casi imposible hace algunos años, ya que no se contaba con las herramientas tecnológicas para hacerlo (Menéndez, 2016).

Existen 2 tipos de monitoreo de red los cuales son:

- **Monitoreo Pasivo:** este enfoque se basa en obtener datos a partir de recolectar y analizar el tráfico que circula por la red. Se usan diversos dispositivos como sniffers y ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para SNMP, RMON y Netflow. Este enfoque no inyecta tráfico a la red como lo hace el modo activo y es utilizado para identificar las características del tráfico en la red y para contabilizar su uso (Menéndez, 2016).
- **Monitoreo Activo:** este tipo de monitoreo inyecta paquetes de pruebas en una red, centrándose en determinadas aplicaciones con el fin de medir

tiempos de respuesta del aplicativo. Su característica principal es inyectar tráfico en la red y se utiliza principalmente para medir su rendimiento (Menéndez, 2016).

### **Analizador de Paquetes de Red Inalámbrica**

Es un software cuyo objetivo es monitorear, capturar y analizar tramas o paquetes en una red de datos que pueden o no estar dirigidas hacia él, conocido también como Sniffer son los motores para los sistemas de detección de intrusiones. Esta herramienta puede utilizarse tanto con fines educativos como maliciosos, así que se debe actuar con discreción en cuanto se sepa de su operación (Silva, 2017).

### **Usos del Analizador de Tráfico Red**

#### ***Uso Correcto***

- Transformar datos binarios que puedan estar encriptados, entregados por las tramas en información legible o de simple lectura.
- Resolver e identificar problemas existentes en la red monitoreada.
- Descubrir cuellos de botella en la red después de un análisis exhaustivo.
- Identificar tarjetas que han sufrido algún daño o están defectuosas.
- Analizar las operaciones sospechosas de aplicaciones o de cualquiera que se desee.
- Aprender acerca de protocolos de seguridad, entre otras funciones (Silva, 2017).

#### ***Uso Incorrecto***

- Descubrir patrones de usuarios conectados a una red.
- Mapeo y escaneo para saber cómo está distribuida una red.
- Robo de contraseñas e información confidencial de usuarios con fines maliciosos.

- Interceptar mensajes de correo electrónico entre usuarios, entre otras (Silva, 2017).

## Analizadores de Paquetes de Redes Inalámbricas en el Mercado

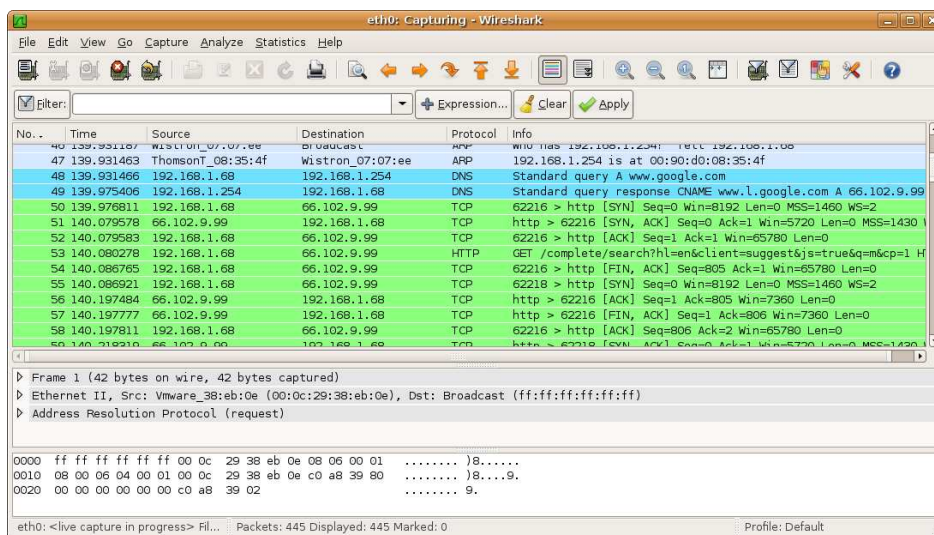
En el mercado existe software libre como software de paga que permite analizar el tráfico dentro de las redes cercanas a las que se tenga acceso de los cuales podemos mencionar los siguientes:

### Wireshark

Wireshark, conocido anteriormente como Ethereal, es un analizador de protocolos que se utiliza para solucionar inconvenientes en redes de datos, también su operación está presente en el desarrollo de software, protocolos y con fines educativos. Posee elementos característicos de un analizador común obtenido en el mercado de forma únicamente hueca (Postigo, 2020). La Figura 8 muestra la interfaz del analizador Wireshark (Imgur, 2015).

### Figura 8

*Interfaz del analizador de protocolos Wireshark.*



*Nota.* Tomado de *Wireshark*, por Imgur., 2015, Imgur (<https://i.imgur.com/272Aehv.png>).

## TShark

Es un analizador de tráfico de red en línea de comando que ayuda a capturar datos de paquetes desde una red o paquetes a ser leídos de un archivo de capturas guardadas anteriormente, se imprime un formulario donde se encuentran decodificados dichos paquetes a la salida estándar o mediante la escritura de los paquetes en un archivo.

Sin otras opciones, TShark funciona como el comando tcpdump y también usa el mismo formato de archivo de captura activa, libpcap. Además, TShark puede detectar, leer y escribir archivos compatibles con Wireshark (Postigo, 2020). A continuación, en la Figura 9 se muestra la interfaz del programa (Wordpress, 2011).

**Figura 9**

*Interfaz Tshark.*

```
C:\>tshark -i2 -q -zhttp.tree -aduration:25 -R "http.host contains 'elmundo'"
Capturing on 3Com EtherLink PCI
96 packets captured
```

HTTP/Packet Counter	value	rate	percent
Total HTTP Packets	402	0,021712	
HTTP Request Packets	202	0,010910	50,25%
GET	199	0,010748	98,51%
POST	3	0,000162	1,49%
HTTP Response Packets	198	0,010694	49,25%
???: broken	0	0,000000	0,00%
1xx: Informational	0	0,000000	0,00%
2xx: Success	187	0,010100	94,44%
200 OK	187	0,010100	100,00%
3xx: Redirection	9	0,000486	4,55%
302 Found	4	0,000216	44,44%
304 Not Modified	5	0,000270	55,56%
4xx: Client Error	2	0,000108	1,01%
400 Bad Request	1	0,000054	50,00%
404 Not Found	1	0,000054	50,00%
5xx: Server Error	0	0,000000	0,00%
Other HTTP Packets	2	0,000108	0,50%

*Nota.* Tomado de *Seguridad y Redes*, por Wordpress., 2011, Wordpress (<https://n9.cl/wk94r>).

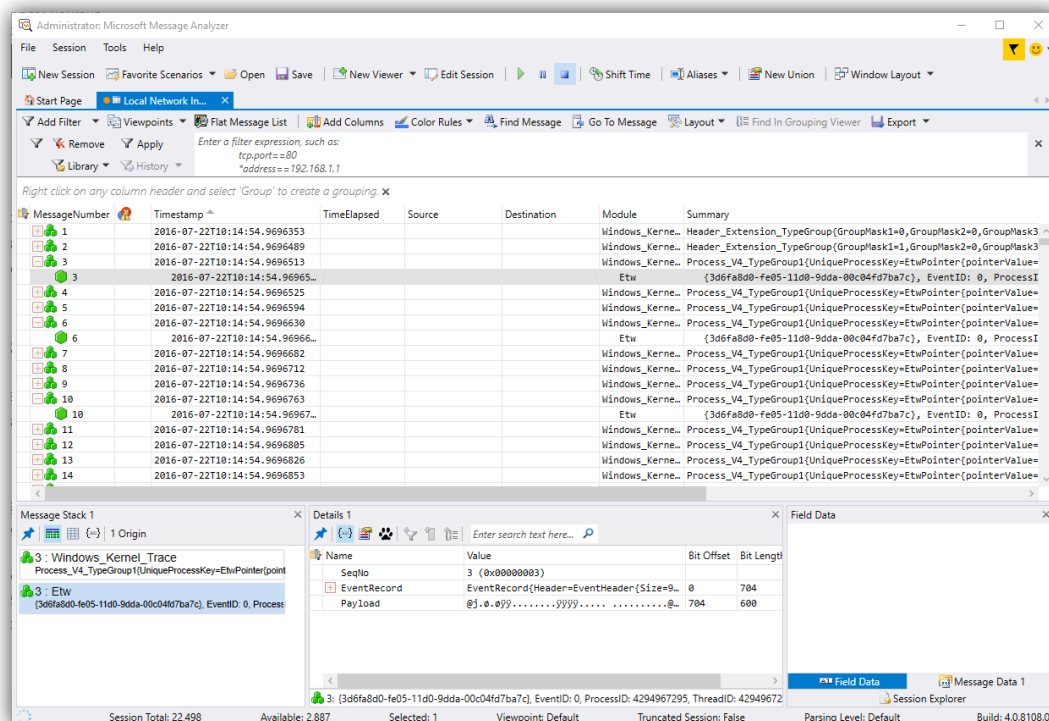
## Microsoft Message Analyzer

Es una aplicación orientada a expertos de redes y administradores de sistemas desarrollados para permitir capturar los paquetes de su red local en tiempo real, listarlos

y analizar el tráfico según los diferentes protocolos (Postigo, 2020). A continuación en la Figura 10 se muestra el interfaz del programa (Imgur, 2015).

**Figura 10**

*Interfaz del programa Microsoft Message Analyzer.*



*Nota.* Tomado de *Microsoft Message Analyzer*, por *Imgur.*, 2015, *Imgur* (<https://i.imgur.com/04r7Rd1.png>).

### **Tcpdump**

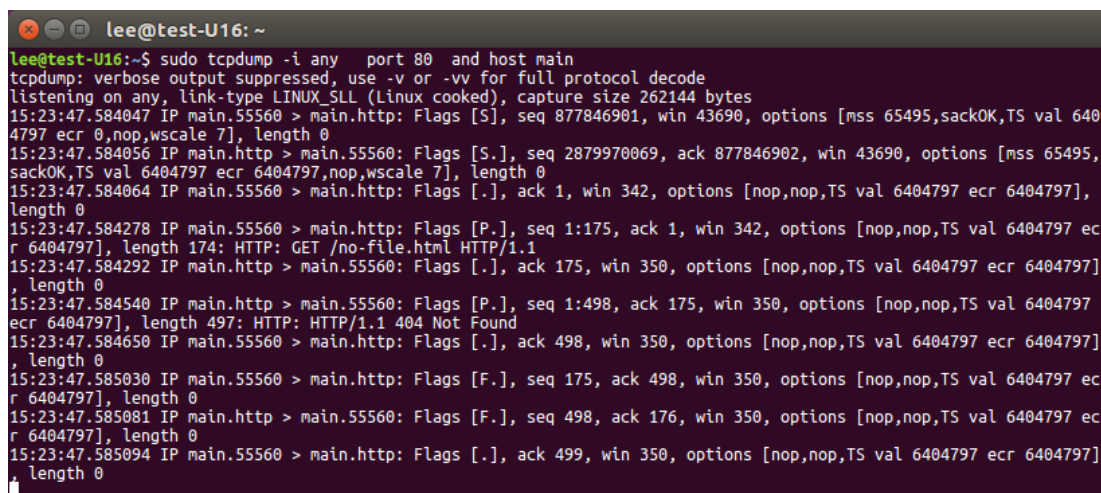
Tcpdump es una herramienta implementada en línea de comandos cuyo objetivo principal es el análisis de tráfico en una red en específico. Este programa permite capturar y mostrar los paquetes transmitidos en tiempo real y que son transmitidos y recibido por el ordenador conectado (Postigo, 2020).

En la Figura 11 se muestra la ejecución del programa tcpdump en la pantalla de comandos (Imgur, 2015).



Figura 11

Ejecución del programa *tcpdump*.



```

lee@test-U16: ~
lee@test-U16:~$ sudo tcpdump -i any port 80 and host main
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
15:23:47.584047 IP main.55560 > main.http: Flags [S], seq 877846901, win 43690, options [mss 65495,sackOK,TS val 6404797 ecr 0,nop,wscale 7], length 0
15:23:47.584056 IP main.http > main.55560: Flags [S.], seq 2879970069, ack 877846902, win 43690, options [mss 65495,sackOK,TS val 6404797 ecr 6404797,nop,wscale 7], length 0
15:23:47.584064 IP main.55560 > main.http: Flags [S.], ack 1, win 342, options [nop,nop,TS val 6404797 ecr 6404797], length 0
15:23:47.584278 IP main.55560 > main.http: Flags [P.], seq 1:175, ack 1, win 342, options [nop,nop,TS val 6404797 ecr 6404797], length 174: HTTP: GET /no-file.html HTTP/1.1
15:23:47.584292 IP main.http > main.55560: Flags [S.], ack 175, win 350, options [nop,nop,TS val 6404797 ecr 6404797], length 0
15:23:47.584540 IP main.http > main.55560: Flags [P.], seq 1:498, ack 175, win 350, options [nop,nop,TS val 6404797 ecr 6404797], length 497: HTTP: HTTP/1.1 404 Not Found
15:23:47.584650 IP main.55560 > main.http: Flags [S.], ack 498, win 350, options [nop,nop,TS val 6404797 ecr 6404797], length 0
15:23:47.585030 IP main.55560 > main.http: Flags [F.], seq 175, ack 498, win 350, options [nop,nop,TS val 6404797 ecr 6404797], length 0
15:23:47.585081 IP main.http > main.55560: Flags [F.], seq 498, ack 176, win 350, options [nop,nop,TS val 6404797 ecr 6404797], length 0
15:23:47.585094 IP main.55560 > main.http: Flags [S.], ack 499, win 350, options [nop,nop,TS val 6404797 ecr 6404797], length 0

```

*Nota.* Tomado de *Tcpdump*, por *Imgur.*, 2015, *Imgur* (<https://i.imgur.com/QOpceNO.png>).

## Herramientas Utilizadas

### *Driver Ndis Wifi*

Acrylic es una herramienta disponible para Windows que permite capturar el tráfico, para esto el programa instala un driver propio para poner en modo monitor al dispositivo de red. El instalar Acrylic da una compatibilidad de forma automática con Wireshark, TShark y Cain & Abel (Security, 2020).

Dentro de todas las funcionalidades existentes en el software de análisis, destacan las siguientes:

- **Visualización de redes:** información SSID de las redes Wi-Fi propagadas en el medio.
- **Clientes:** identificación de variedad de dispositivos con su respectiva dirección MAC asociada (BSSID) conectados a las redes Wi-Fi y en modo monitor.
- **Cifrado:** cifrado WEP, WPA, WPA2.

- **Autenticación:** información sobre redes que se encuentran abiertas, WEP, Enterprise (802.1X).
- **Nivel de señal:** gráficas de señal correspondientes a las redes Wifi y los clientes asociados a esta red.
- **Canales:** descripción de la distribución de redes Wifi que ocupan los canales en 2.4Ghz y 5Ghz.
- **GPS:** uso de soporte GPS para ubicación geo-referencial de los equipos.
- **Google Maps:** generación de ficheros KML/KMZ que permiten hacer uso de las herramientas de google maps o google earth.
- **Inventario:** asignación de identificadores simples o nombres a los dispositivos conocidos por la red con una limitante de 10 resultados (Security, 2020).

### ***Lb Link Blwn150ah***

El adaptador inalámbrico USB BL-WN150AH, permite la interconexión entre una PC o portátil a una red inalámbrica y así acceder a Internet de alta velocidad. Usando la tecnología 1-stream basada en la tecnología 802.11n, este producto ofrece una mejor señal inalámbrica de la tecnología 802.11g existente. Equipado con una antena desmontable de 5dBi, puede aumentar su rango de señal y velocidad y por consiguiente puede conseguir una mejor experiencia al momento de conectarse a Internet, como descargas, juegos, streaming de video y audio, etc., esta información se encuentra en la sección de anexos, el anexo A. A continuación se muestra al adaptador LB-Link en la Figura 12 (Sincables, 2018).

### **Figura 12**

*Adaptador usb LB-Link Bl-wn150ah.*



*Nota.* Tomado de *LB-Link Bl-wn150ah*, por Sincables., 2018, Sincables (<https://sincables.com.ec/wp-content/uploads/2018/11/BL-WN150AH-2.jpg>).

### ***Tarjeta de Red TL-wn722n***

La tarjeta es un adaptador USB Inalámbrico de alta ganancia de la cual se puede ver en la Figura 13 (TP-Link, 2020), también se destacan las siguientes características:

- Velocidad inalámbrica que puede tener hasta 150 Mbps reuniendo así la mejor experiencia para la difusión de videos o las llamadas por Internet.
- Encriptación lograda por el botón de QSS que permite resguardar los datos de la red inalámbrica.
- 4dBi antena desmontable, para fortalecer la potencia de la señal del adaptador USB.
- Soporta Windows 10/8.1/8/7/XP, Mac OS X 10.8-10.14, Mac OS X 10.8-10.14, Linux OS (TpLink, 2015).

Esta información se encuentra en la sección de anexos, el anexo B.

### **Figura 13**

*Adaptador usb TL-wn722n.*



*Nota.* Tomado de *TL-wn722n*, por Tp-Link., 2018, Tp-Link (<https://n9.cl/eed9o>).

### ***AirPcap Nx***

AirPcap Nx es un adaptador compatible con sistemas operativos de Windows el cual permite la captura e inyección de paquetes en las redes 802.11a/b/g/n (Riverbed, 2009), sus características principales son:

- Integración completa con Wireshark y Cascade Pilot para un análisis, visualización, desglose e informes completos del tráfico WLAN.
- Captura de tráfico 802.11n en canales de 20 MHz y 40 MHz.
- Captura de paquetes 802.11a, b, g en canales de 20MHz.
- Inyección de paquetes 802.11a / b / g / n a todas las velocidades.
- Información de radio por paquete.
- Resolución de marca de tiempo de microsegundos.
- Soporte para captura multicanal simultánea en un solo, archivo de seguimiento combinado utilizando varios adaptadores AirPcap Nx y agregación exclusiva de múltiples canales tecnología.
- Las API de AirPcap y WinPcap se proporcionan para la creación o extensión de sus propias herramientas de laboratorio.

### ***Acrylic Wi-fi Professional***

Dentro de los productos que ofrece Acrylic la versión seleccionada fue Wi-Fi profesional ya que es ideal para uso personal, el costo de una licencia por un año es de 20 dólares.

Una característica importante de esta versión es el modo monitor que permite capturar tramas de datos, administración y control mediante un driver NDIS que soporta varios modelos (Security, 2020).

Dependiendo del fabricante del adaptador de red el controlador de Acrylic varia su desempeño. Por ejemplo, de acuerdo de acuerdo a la información acerca de dispositivos compatibles con acrylic la marca Atheros presenta buena compatibilidad mientras que la marca Ralink limitada (Security, 2020).

### ***Tarjetas compatibles en modo monitor a travez del controlador de acrylic***

A continuación en la Tabla 2 se muestra a las tarjetas compatibles con el software acrylic para ser usadas en modo monitor.

**Tabla 2**

*Tarjetas compatibles con acrylic.*

<b>Modelo</b>	<b>20</b>	<b>40</b>	<b>80</b>	<b>SNR</b>	<b>2.4</b>	<b>5</b>	<b>Compatibilidad</b>
Broadcom BCM43236	SI	-	-	-	b/g/n	a/n	Muy buena
Linksys AE2500 N600	SI	-	-	-	b/g/n	a/n	Muy buena
Asus USB-AC53 (versión Nano NO soportada)	SI	-	-	-	b/g/n	a/n/ac	Muy buena
NetGear A6200	SI	-	-	-	b/g/n	a/n/ac	Muy buena
D-Link DWA-182 Revision A1 a/g/n/ac	SI	-	-	-	b/g/n	a/n/ac	Muy buena
TP-LINK TL-WN722N v1 (v2 NO soportada)	SI	-	-	-	b/g/n	a/n	Buena
Ralink RT2870/3070 / Alpha	SI	-	-	-	b/g/n	a/n	Limitada

Aircap Classic	SI	-	-	SI	b/g/n	-	Buena
Aircap Tx	SI	-	-	SI	b/g/n	-	Buena
Aircap Nx	SI	-	-	SI	b/g/n	a/n	Buena

## Python

Es un lenguaje de programación potente y muy utilizada ya que es fácil de aprender. Entre sus características posee estructuras de datos de alto nivel y un enfoque sencillo pero efectivo de la programación orientada a objetos. Su sintaxis elegante, los tipos de datos dinámicos y el hecho de ser un lenguaje interpretado hacen de Python un lenguaje ideal para la creación de scripts y el desarrollo rápido de aplicaciones en todo tipo de áreas y plataformas (Rojas, 2019).

El intérprete de Python puede ampliarse fácilmente con nuevas funciones y tipos de datos implementados en C o C++ (u otros lenguajes accesibles desde C). Python es también adecuado como lenguaje de extensión de aplicaciones (Rojas, 2019).

### **Scapy de Python**

Es una herramienta descrita en Python que nos sirve para crear y manipular paquetes, escanear, funciones de sniffer, creación de gráficas 2D/3D/ Pdf, passive OS fingerprinting, tracers gráficos, además, podemos crear herramientas escritas en Python usando scapy. Posee funciones parecidas a tllscan, nmap, hping, queso, p0f, xprobe, arping, arp-sk, ARPSpoof y firewalk (Rojas, 2019).

Todo mediante línea de comandos, es integrable en Python, programable, versátil y flexible. Obtendremos solo los datos que queramos y todo lo complejo que deseemos (Rojas, 2019).

### ***Función Sniff de Scapy***

La función a sniff de scapy permite especificar varias opciones: opción offline permite leer archivos .pcapng y se caracteriza por un bajo consumo de memoria, la opción prn permite indicar el nombre de una función para extraer información de interés de los paquetes y la opción stop filter permite parar la lectura de paquetes al cumplirse una condición especificada.

### ***Base de Datos***

Una base de datos es simplemente una colección de datos en una estructura definida. Una base de datos es un lugar en el que los datos son almacenados y organizados. La palabra “relacional” significa que los datos almacenados en el conjunto de datos son organizados en forma de tablas. Cada tabla se relaciona de alguna manera. Si el software no es compatible con el modelo de datos relacionales, simplemente se llama DBMS (Wisborg & Okuno, 2019).

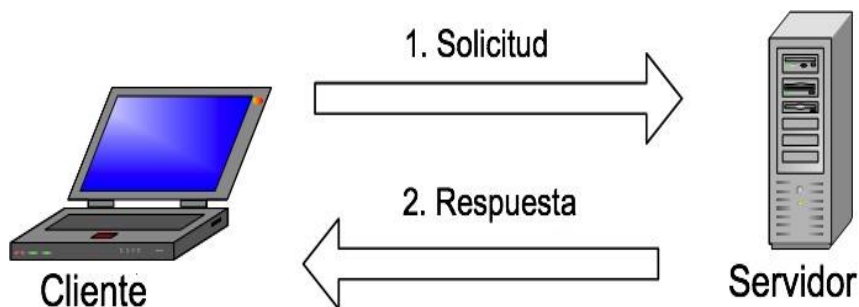
### ***Mysql***

Es un sistema de gestión de bases de datos relacionales de código abierto (RDBMS, por sus siglas en inglés) con un modelo cliente-servidor. RDBMS es un software o servicio utilizado para crear y administrar bases de datos basadas en un modelo relacional (Wisborg & Okuno, 2019).

En la Figura 14 se muestra la función del sistema de gestión de datos MySQL (Hostinger, 2019).

### **Figura 14**

*Gestión de datos de MySQL.*



*Nota.* Tomado de *Cómo funciona MySQL*, por Hostinger., 2019, Hostinger (<https://n9.cl/98o1z>).

La Figura anterior detalla la estructura básica cliente-servidor. Uno o más dispositivos (clientes) se conectan a un servidor a través de una red específica. Cada cliente puede realizar una solicitud desde la interfaz gráfica de usuario (GUI) en sus pantallas, y el servidor producirá un output requerido, siempre que ambas partes entiendan la instrucción. Sin profundizar demasiado en temas técnicos, los procesos principales que tienen lugar en un entorno MySQL son los mismos, y son:

- MySQL crea una base de datos para almacenarlos y manipularlos, definiendo una relación de cada tabla.
- Los clientes pueden realizar solicitudes escribiendo instrucciones SQL específicas en MySQL.
- La aplicación del servidor responderá con la información solicitada y esta aparecerá frente a los clientes (Wisborg & Okuno, 2019).



## Capítulo III

### **Desarrollo del Aplicativo para Caracterizar Tramas 802.11**

El desarrollo del programa se lo realizó mediante la IDE de Python con sus librerías y el controlador de Acrylic, el cual permite capturar las tramas 802.11 y visualizarlas mediante un análisis del tipo y subtipo de trama.

Inicialmente el programa permite realizar la conexión a la base de datos en la cual se almacenan los datos obtenidos mediante la captura para su posterior análisis, adicionalmente el programa permite visualizar las tarjetas de red con las que se va a realizar la captura que son compatibles con el sistema operativo de Windows y seleccionarlas para iniciar la ejecución del programa.

El programa permite visualizar tablas con la información procesada y el usuario podrá seleccionar entre la clasificación total de tramas, los dispositivos asociados a las redes, así como también el detalle de los datos capturados por cada subtipo de trama.

### **Diseño del Aplicativo para Caracterizar Tramas 802.11**

El objetivo principal del aplicativo desarrollado es capturar e indagar tramas 802.11, así como extraer aquellos parámetros más relevantes para su estudio, es por cuanto para su desarrollo e implementación se utilizó Python. En el programa se visualizará en tablas los datos más relevantes de cada red y sus diferentes tipos de tramas, así como un resumen porcentual de los paquetes capturados por cada BSSID o mac de dispositivos, además de un resumen del total de tramas de administración, control y datos.

### **Controladores y Modo Monitor**

Con ayuda del driver NDIS acrylic incluido en el software Acrylic Wi-fi Professional se genera automáticamente una interfaz emulada que inicia con el nombre

“Acrylic” y está configurada en modo monitor para capturar tramas de administración, control y datos.

En este paso podemos comprobar la información acerca de comportamiento de los adaptadores de red. Como se puede observar en la Figura 15 la tarjeta Atheros AR9271 captura paquetes en diferentes canales.

### Figura 15

*Canales de captura de paquetes de tarjeta Atheros.*

Channel	Info
7	Beacon frame, SN=1747, FN=0, Flags=.....C, BI=100, SSID=NETLIFE-C
4	Beacon frame, SN=1806, FN=0, Flags=.....C, BI=100, SSID=NETLIFE-L
6	Beacon frame, SN=202, FN=0, Flags=.....C, BI=98, SSID=NETLIFE-Car
1	Beacon frame, SN=203, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT[
2	Beacon frame, SN=208, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT[
7	Beacon frame, SN=209, FN=0, Flags=.....C, BI=98, SSID=NETLIFE-Car
1	Beacon frame, SN=2255, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT
2	Beacon frame, SN=2262, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT
8	Beacon frame, SN=2316, FN=0, Flags=.....C, BI=98, SSID=NETLIFE-Ce
6	Beacon frame, SN=2571, FN=0, Flags=.....C, BI=100, SSID=FIBRAMAX
7	Beacon frame, SN=2573, FN=0, Flags=.....C, BI=100, SSID=FIBRAMAX
1	Beacon frame, SN=2928, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT
7	Beacon frame, SN=3443, FN=0, Flags=.....C, BI=100, SSID=NETLIFE-C
8	Beacon frame, SN=3448, FN=0, Flags=.....C, BI=100, SSID=NETLIFE-C
6	Beacon frame, SN=3578, FN=0, Flags=.....C, BI=98, SSID=NETLIFE-Ce
7	Beacon frame, SN=3582, FN=0, Flags=.....C, BI=98, SSID=NETLIFE-Ce
2	Beacon frame, SN=3634, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT
6	Beacon frame, SN=4040, FN=0, Flags=.....C, BI=100, SSID=NETLIFE-C
5	Beacon frame, SN=882, FN=0, Flags=.....C, BI=100, SSID=FIBRAMAX _
1	Beacon frame, SN=901, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT[
2	Beacon frame, SN=910, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT[
3	Beacon frame, SN=911, FN=0, Flags=.....C, BI=100, SSID=SOFIA_CNT[
6	Beacon frame, SN=937, FN=0, Flags=.....C, BI=98, SSID=NETLIFE-Car

Mientras que en la Figura 16 se puede observar que la información acerca de los canales no está presente. A pesar de esto se puede extraer información importante como se mostrará en otra sección.

### Figura 16

*Canales de captura de paquetes de la tarjeta Ralink.*

```

Channel Info
802.11 Block Ack, Flags=.....C
802.11 Block Ack, Flags=.....C
Acknowledgement, Flags=.....C
Acknowledgement, Flags=.....C
Acknowledgement, Flags=.....C
Beacon frame, SN=1539, FN=0, Flags=.....C, BI=100, SSID=
Beacon frame, SN=1650, FN=0, Flags=.....C, BI=100, SSID=
Clear-to-send, Flags=.....C
Clear-to-send, Flags=.....C
Clear-to-send, Flags=.....C
Clear-to-send, Flags=.....C

```

### **Herramientas de Captura**

Se instaló la versión de Wireshark 3.4.0, en esta viene incluido los programas tshark y dumpcap que se ejecutaran desde la línea de comandos o desde Python.

En la Figura 17 se puede observar una lista de las interfaces generadas mediante el comando: tshark -D, esta información es necesaria para filtrar las interfaces que inicien con el nombre airpcap y que se utilizaran para capturar tramas en modo monitor.

### **Figura 17**

*Lista de interfaces encontradas mediante tshark.*

```

(venv) C:\Users\efota\Desktop\Enviar_version4>tshark -D
1. \Device\NPF_{D876529B-458F-4E86-9003-75E354738B4F} (Ethernet 3)
2. \Device\NPF_{D4DD0489-55BA-4DF5-9C5C-9A1D0406C6BB} (Conexión de área local* 8)
3. \Device\NPF_{7C5A0860-7212-4543-9290-3FA931FFFCFC} (Conexión de red Bluetooth)
4. \\.\airpcap13_{50621ECD-834D-4668-9809-E629F2246094}-\{CD3F5F0A-AEE2-450E-850E-A40BA3F3C7C2}-0000 (Acrylic NDIS Microsoft Wi-Fi Direct Virtual Adapter)
5. \\.\airpcap12_{E660A492-A4CB-4678-AADD-2F502B368EB1}-\{CD3F5F0A-AEE2-450E-850E-A40BA3F3C7C2}-0000 (Acrylic NDIS Atheros AR9271 Wireless Network Adapter)
6. \\.\airpcap11_{92F6FBF4-6AC4-4E33-9F68-3870099918D0}-\{CD3F5F0A-AEE2-450E-850E-A40BA3F3C7C2}-0000 (Acrylic NDIS TP-Link Wireless USB Adapter)
7. \\.\airpcap10_{DC344405-2F6A-4A2D-A0F5-31A040E62131}-\{CD3F5F0A-AEE2-450E-850E-A40BA3F3C7C2}-0000 (Acrylic NDIS 802.11n USB Wireless LAN Card)

```

Mediante Dumcap se realiza la captura con el siguiente comando ejecutado desde Python con el modulo os: dumpcap -i <nombre\_interfaz> -b filesize:<tamaño> -w <nombre\_archivo.pcapng>. Es necesario indicar el nombre de la interfaz de captura en modo monitor, el tamaño máximo y el nombre del archivo pcapng.

El tamaño máximo seleccionado fue de 1 KB ya que por cada archivo se generan entre 6 y 8 paquetes.

Posteriormente cada archivo .pcapng creado es leído y procesado por el hilo packet handler.

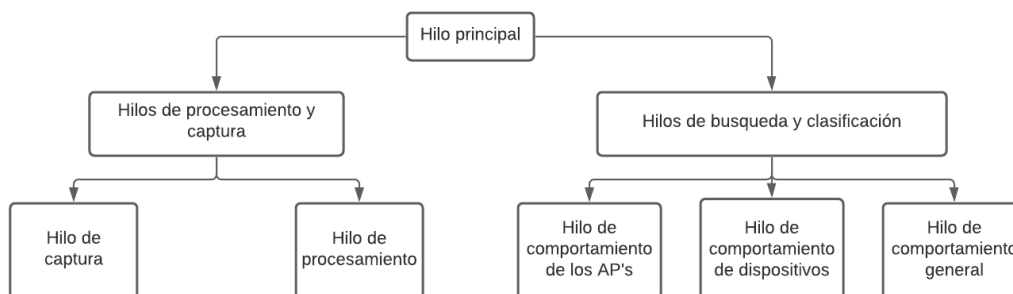
## Estructura del Programa

El programa se ejecuta mediante un hilo principal el cual contiene a los hilos de captura y procesamiento los cuales se encargan de realizar la captura de las tramas para realizar un procesamiento paralelo; y el segundo hilo que se ejecuta con el hilo principal es el de búsqueda y clasificación, el cual se encarga de realizar la búsqueda de datos y clasificarlos mediante el SSID en las diferentes tablas de visualización.

A continuación en la Figura 18 se muestra un esquema general de la estructura del programa.

### Figura 18

*Estructura del programa.*



## Diseño de la Interfaz Gráfica para la Captura de Tramas y Procesamiento de Datos

### **Diagrama de Bloques del Aplicativo**

Todas las clases cuyo nombre inicie con “Thread” heredan los métodos de la clase Qthread que permiten comunicarse entre hilos de diferentes clases o el hilo principal con ayuda de señales.

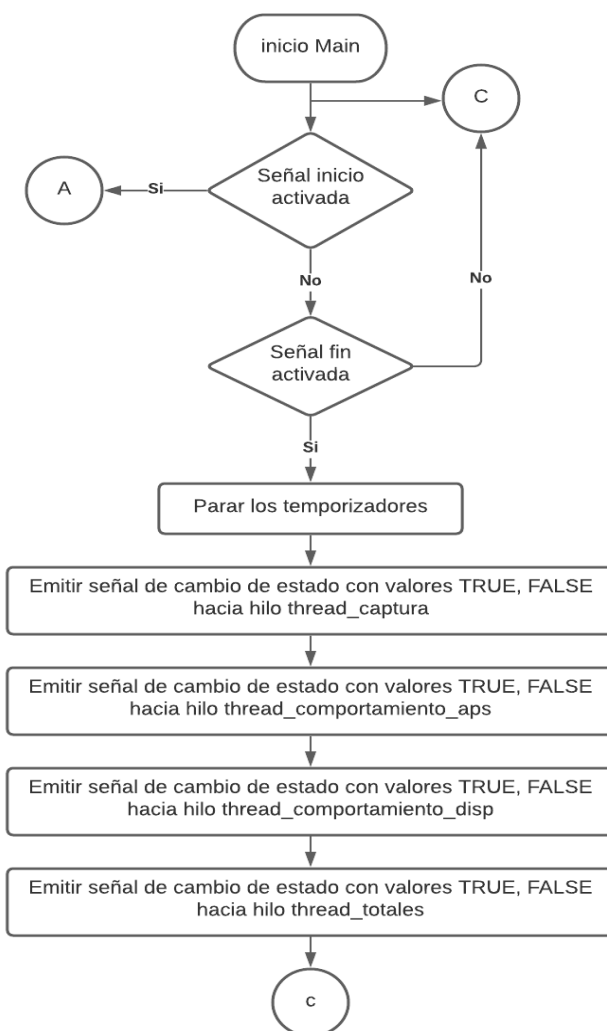
Las señales son el mecanismo que utiliza el paquete Pyqt5 para enviar información hacia métodos definidos por el usuario que permiten cambiar el estado de variables y objetos tanto en la interfaz gráfica como en otros hilos.

“Main” es el hilo principal que se crea al correr el programa, este hilo se encargará de abrir conexiones con la base de datos, buscar interfaces de tipo “acrylic” y está a la espera de que el usuario presione el botón de captura para iniciar todos los hilos que se explicaran posteriormente e iniciar temporizadores si se requieren.

Si el usuario presiona el botón finalizar se ejecutará una función que finaliza de manera segura todos los hilos creados y para los temporizadores que estén activos. A continuación en la Figura 19 se denota el diagrama de flujo de la función “Main”.

**Figura 19**

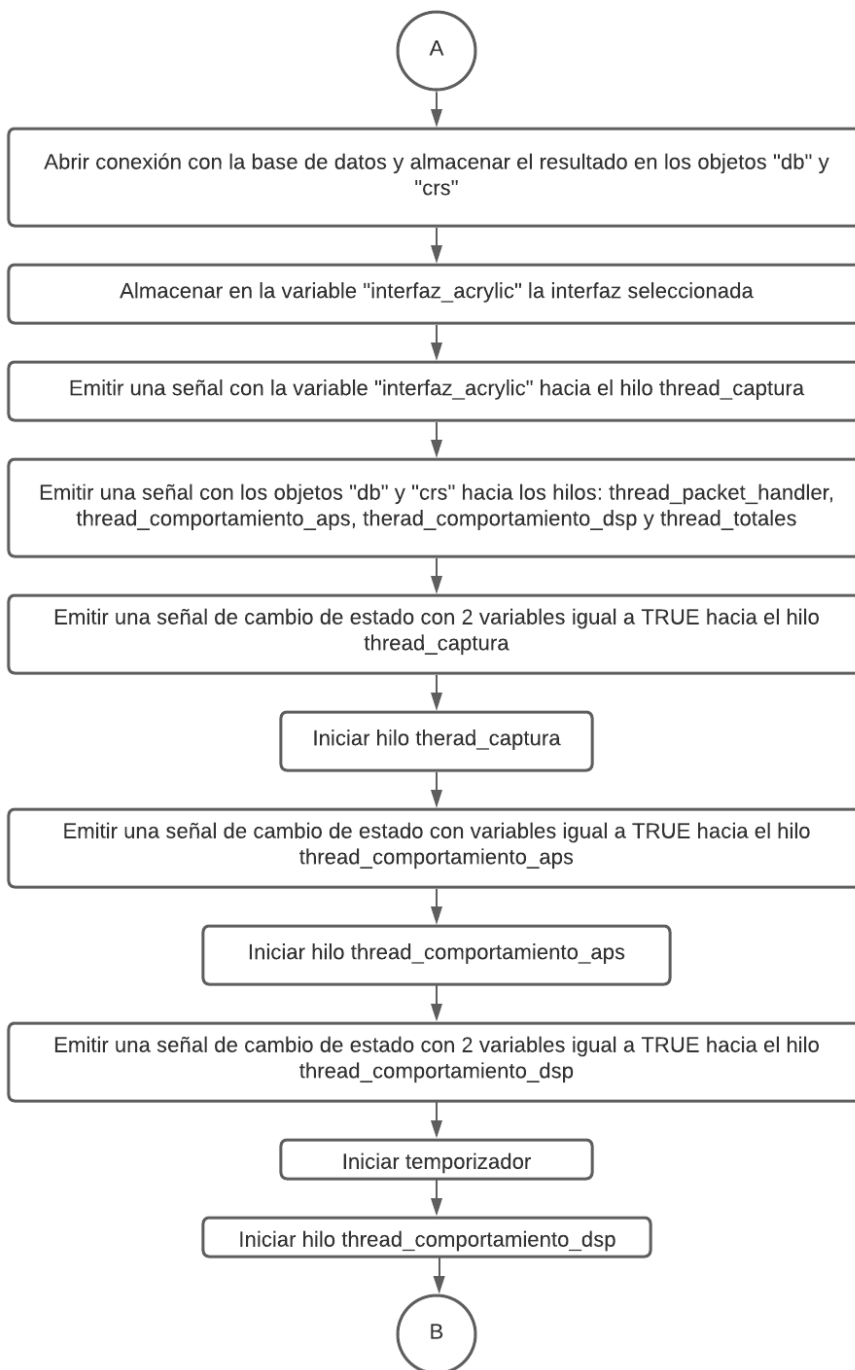
*Diagrama de Flujo de la función Main.*



Se muestra la continuación del diagrama de flujo de la función "Main" en la Figura 20.

### Figura 20

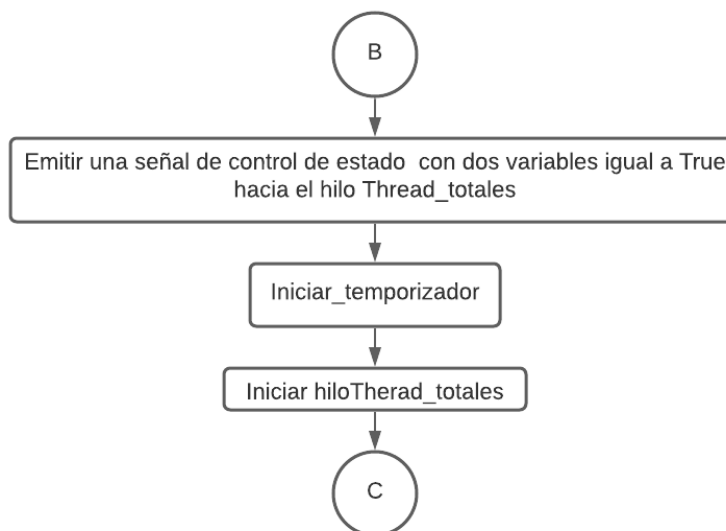
*Continuación de la función Main.*



En la Figura 21 se denota la continuación del diagrama de flujo de la función “Main”.

### Figura 21

*Continuación de la función Main.*



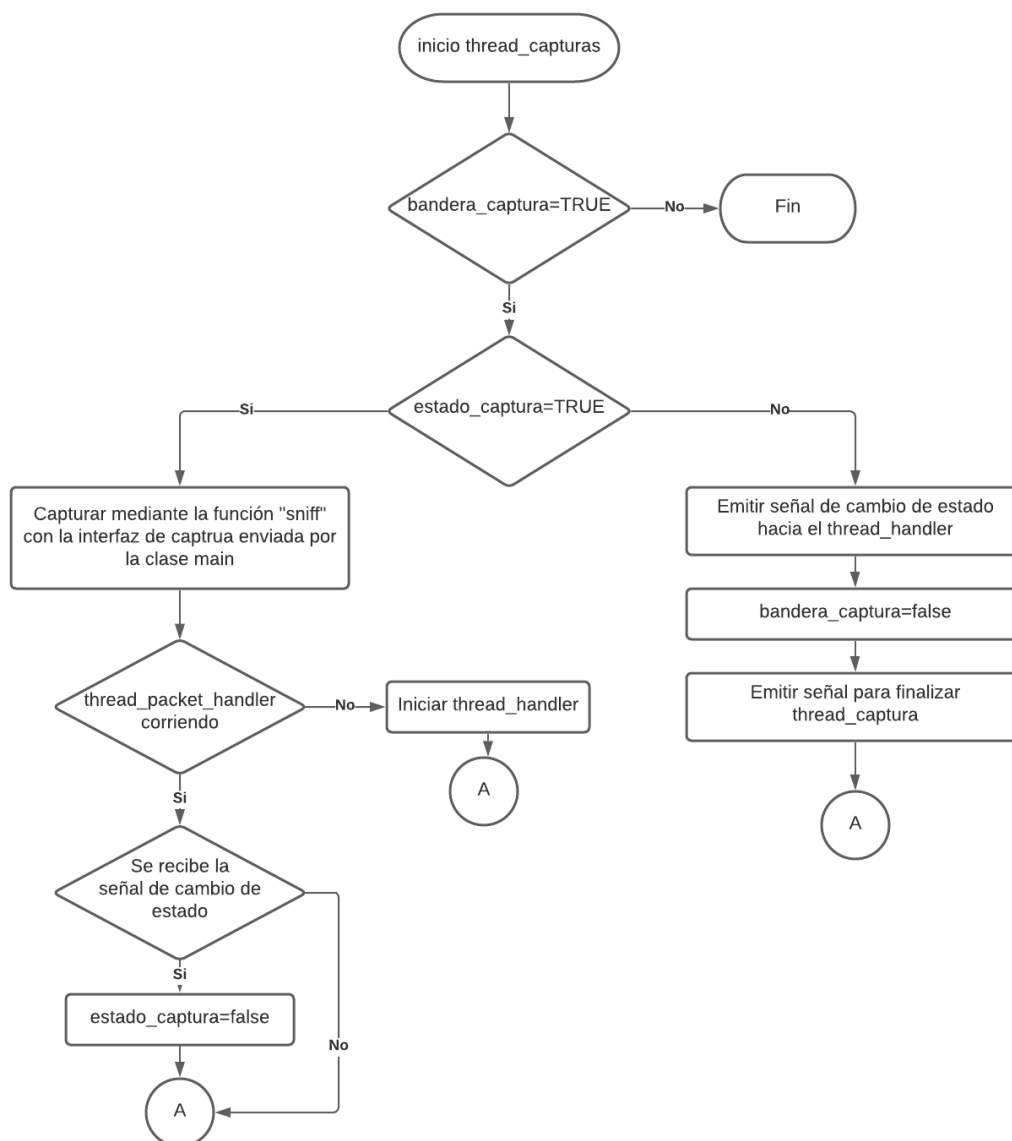
### ***Etapa de Captura***

El hilo “thread\_captura” lee constantemente las variables estado captura y bandera captura para determinar si debe finalizar con el bucle y emitir una señal para finalizar con el hilo de captura.

A continuación la Figura 22 se muestra el diagrama de flujo de la función “thread\_capturas” y sus condiciones.

### Figura 22

*Diagrama de flujo de la función thread\_capturas.*



Este hilo utiliza una cola compartida que permite almacenar los paquetes capturados para posteriormente enviar señales al hilo “thread\_handle” que se encargara de procesar esta información. En caso de que el hilo de procesamiento no esté ejecutándose también se encarga de iniciarlo

### ***Etapa de Procesamiento***

El hilo “thread\_packet\_handler” lee todo el tiempo las variables booleanas, “bandera\_handler” que se utiliza para salir del bucle y “estado\_handler” para cerrar un

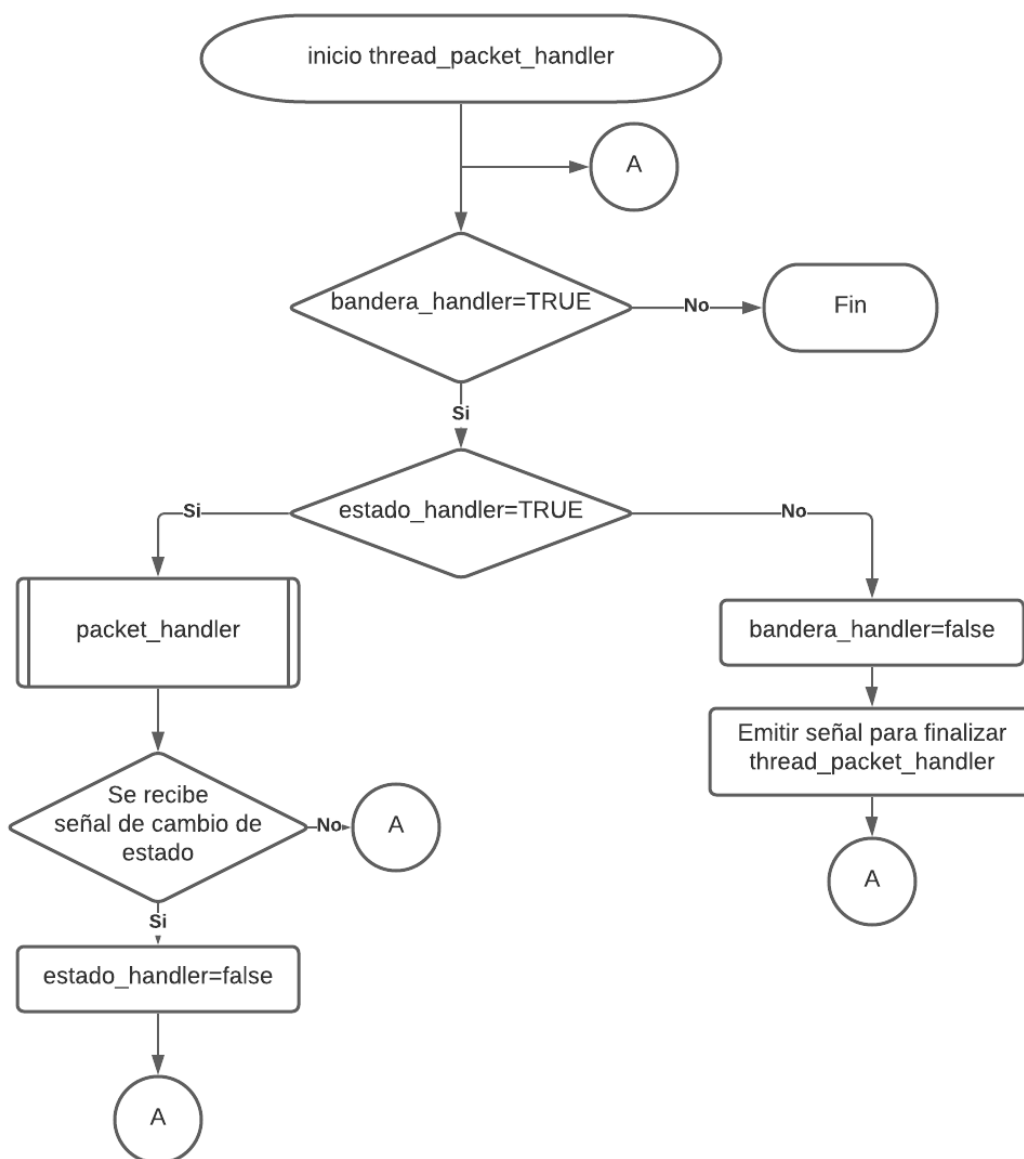


bucle “for” interno el cual ejecuta la función “packet handler” encargada de determinar el “tipo subtipo” de trama e información de interés de los paquetes capturados.

El diagrama de flujo de la función “thread\_packet\_handler” se muestra en la Figura 23 se muestra a continuación.

### Figura 23

*Diagrama de flujo de la función thread\_packet\_handler.*

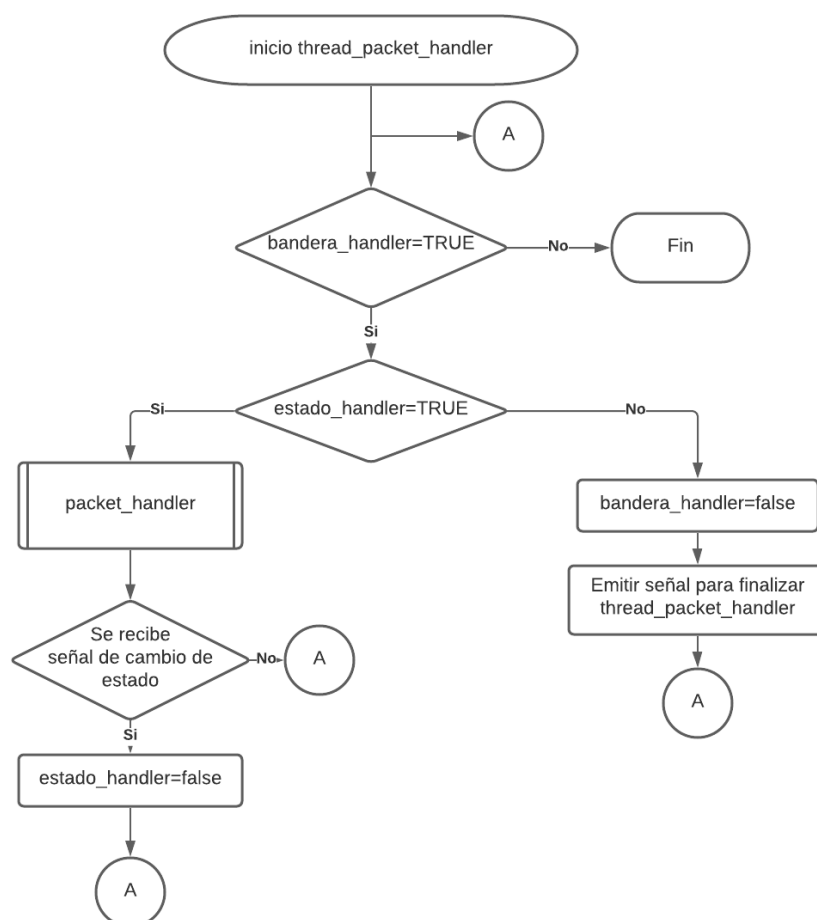


La función “paquet\_handler” permite extraer el subtipo, direcciones MAC de origen y destino, además del tipo de cifrado, encriptación y autenticación. Esta información se almacena en listas que representan los siguientes tipos de tramas: Administración, control y datos.

El diagrama de flujo de la función “packet\_handler” se muestra en la Figura 24 se muestra a continuación.

**Figura 24**

*Diagrama de flujo de la función packet\_handler.*

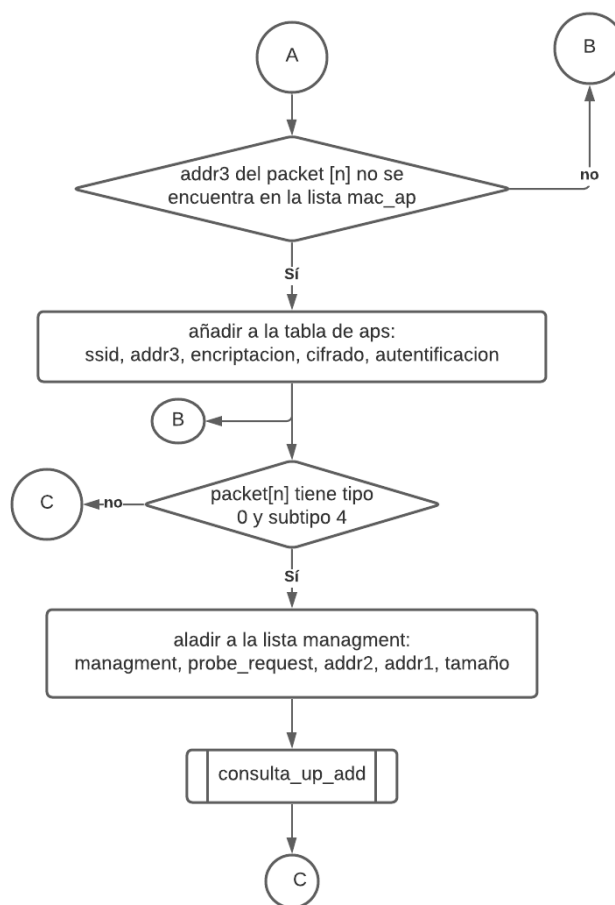


Cuando la lista está completa se llama a la función “consulta\_up\_add” que permite extraer datos de la “tabla\_general”, si existe un registro en el que coinciden las

MAC de origen y destino actualiza la fila correspondiente, caso contrario añade la información en una nueva fila. La primera parte del proceso de extracción de datos se puede ver en la Figura 25 que se muestra a continuación.

**Figura 25**

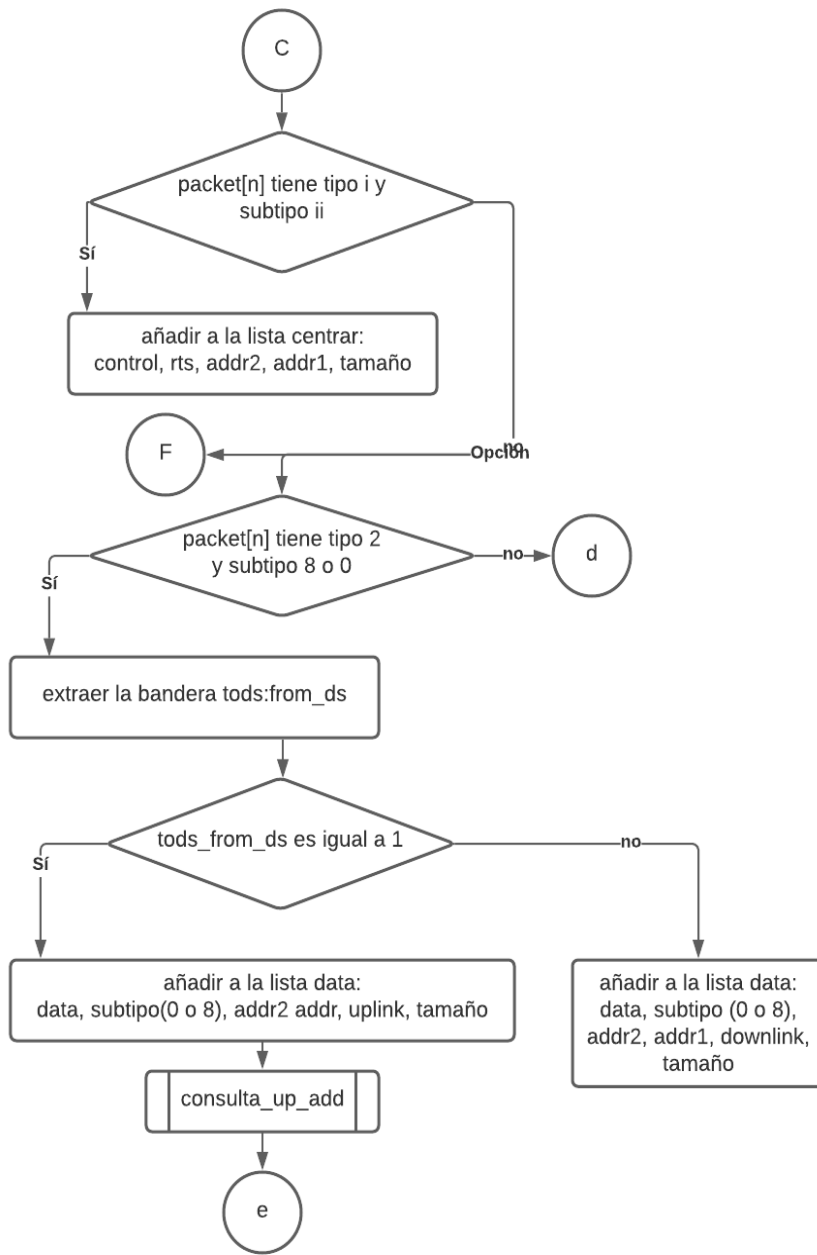
*Diagrama de flujo de la sección de extracción de datos.*



La segunda parte del proceso de extracción de datos se puede ver en la Figura 26 que se muestra a continuación.

**Figura 26**

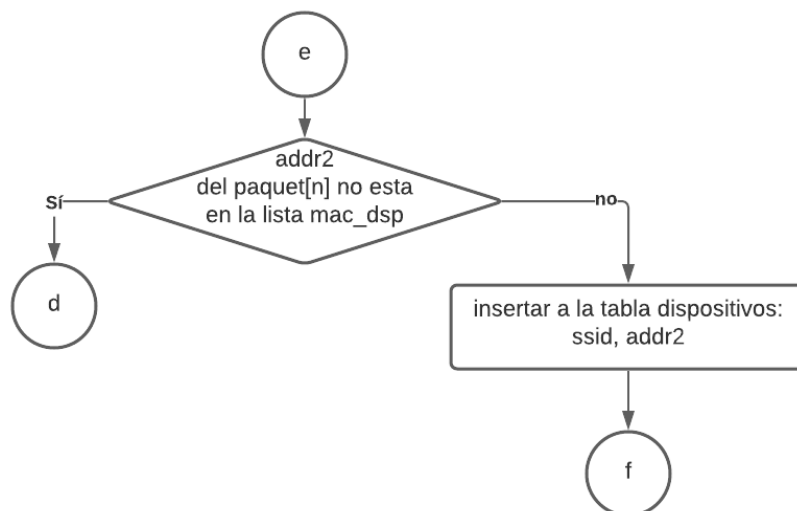
*Diagrama de flujo de la sección de extracción de datos.*



La continuación de la recolección de datos e ingreso en la tabla de dispositivos se puede ver en la Figura 27.

### Figura 27

*Ingreso de datos en la tabla de dispositivos.*

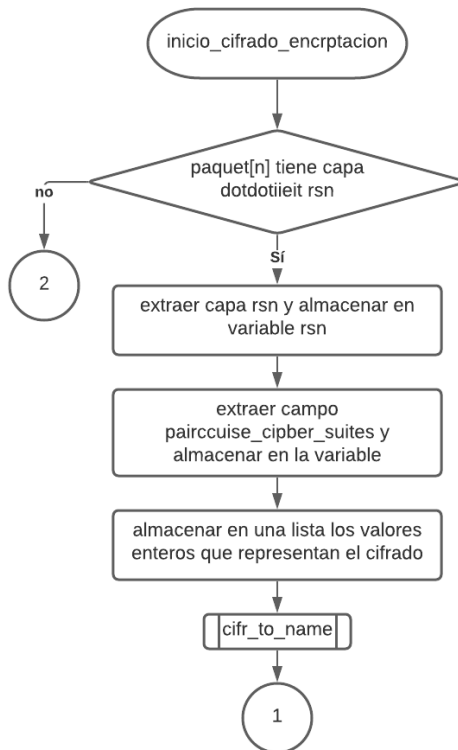


La función “inicio\_cifrado\_encryption” consiste en extraer las capas Dot11EltRSN y Dot11EltMicrosoftwpa mediante el método getlayer del módulo Scapy el cual retorna un objeto que tiene la propiedad “pairwise\_cipher\_suites” para obtener información como el tipo de cifrado y encriptación. Otra propiedad de este objeto es “Akm\_suites” que contiene el tipo de autenticación.

Toda esta información se representa mediante números por lo que se utiliza la función “cifr\_to\_name” para obtener el nombre del tipo de cifrado, encriptación y la función “aut\_to\_name” para obtener el nombre del tipo de autenticación. A continuación en la Figura 28 se muestra el diagrama de flujo de la función “inicio\_cifrado\_encryption”.

### Figura 28

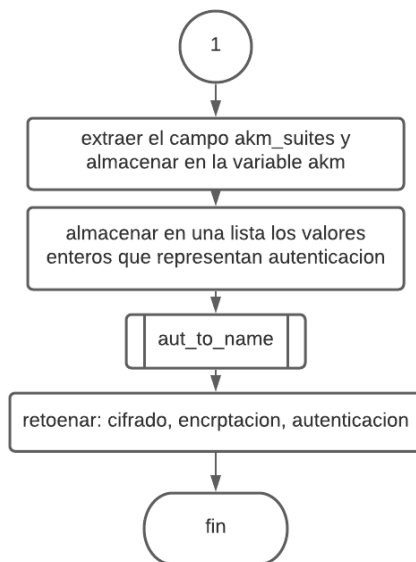
*Diagrama de flujo de la función de inicio, cifrado y encriptación.*



En la Figura 29 se muestra la continuación el diagrama de flujo de la función “inicio\_cifrado\_encrptacion”.

### Figura 29

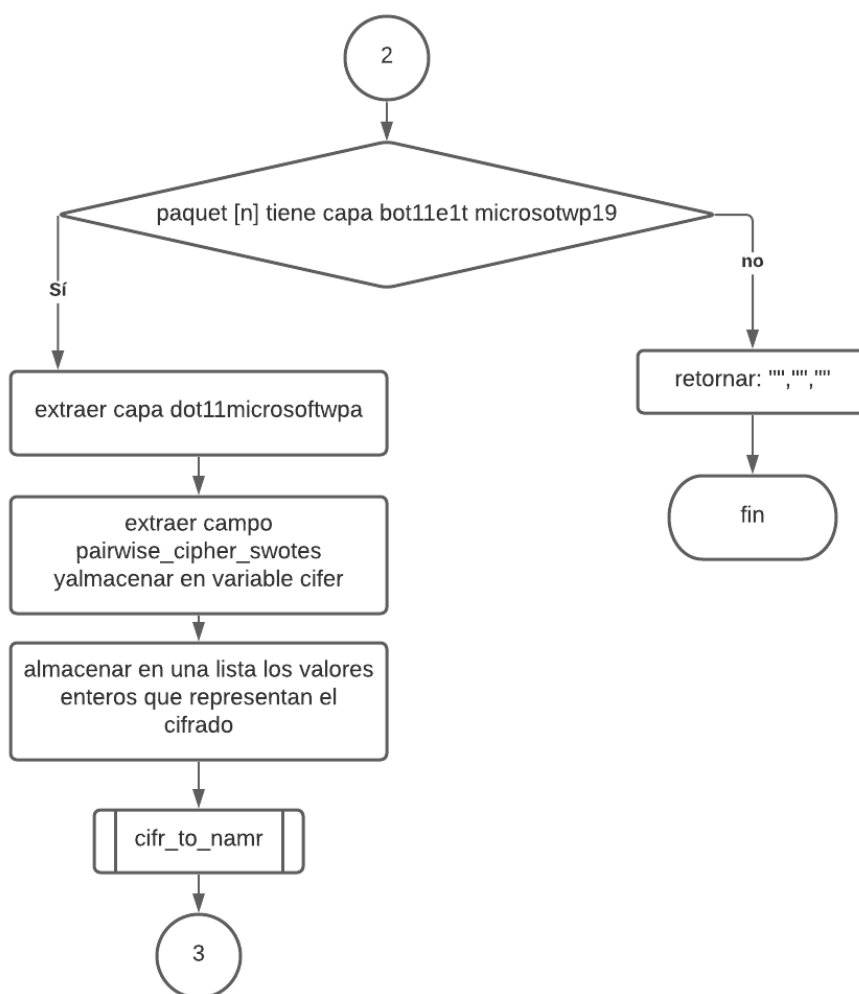
*Continuación de la función de inicio\_cifrado\_encrptacion.*



En la Figura 30 se muestra la continuación el diagrama de flujo de la función “inicio\_cifrado\_encryption”.

### Figura 30

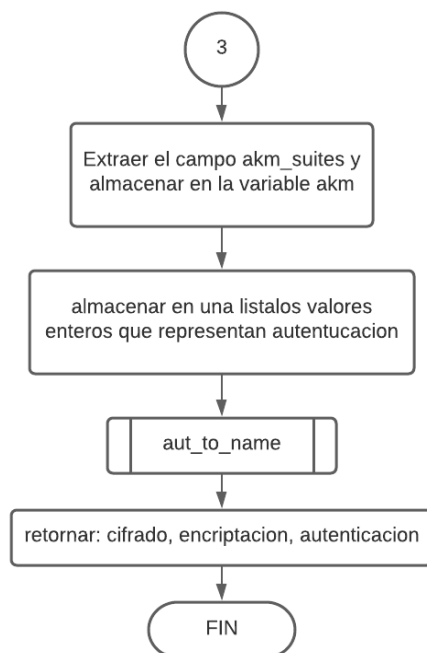
Continuación de la función de inicio\_cifrado\_encryption.



Se extraen los campos correspondientes y se almacenan los valores de autenticación para así enviarlos a la función “aut\_to\_name” y retornar los datos del cifrado, encriptación y autenticación como se muestra en la Figura 31.

### Figura 31

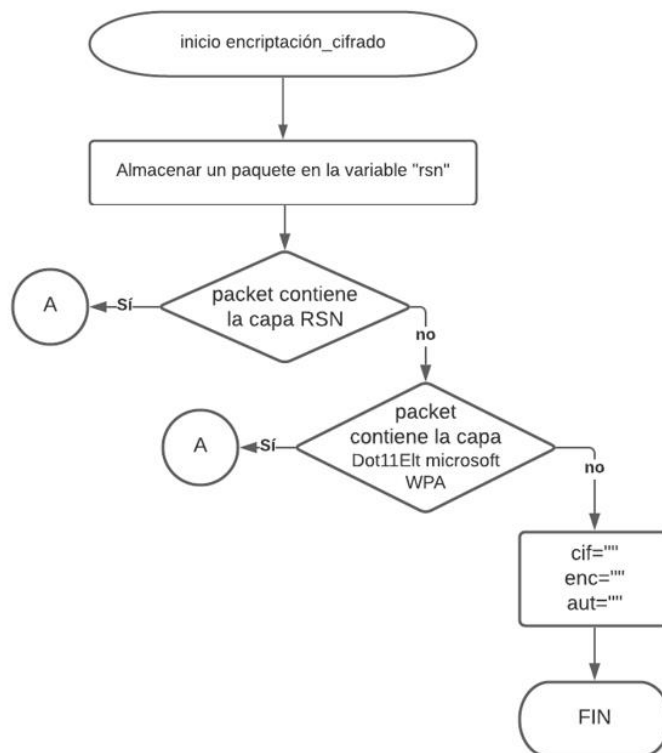
Diagrama del retorno de datos de cifrado, encriptación y autenticación.



En la Figura 32 se muestra el diagrama de flujo de "inicio\_encryptacion\_cifrado".

### Figura 32

*Inicio del diagrama de flujo inicio\_encryptacion\_cifrado.*

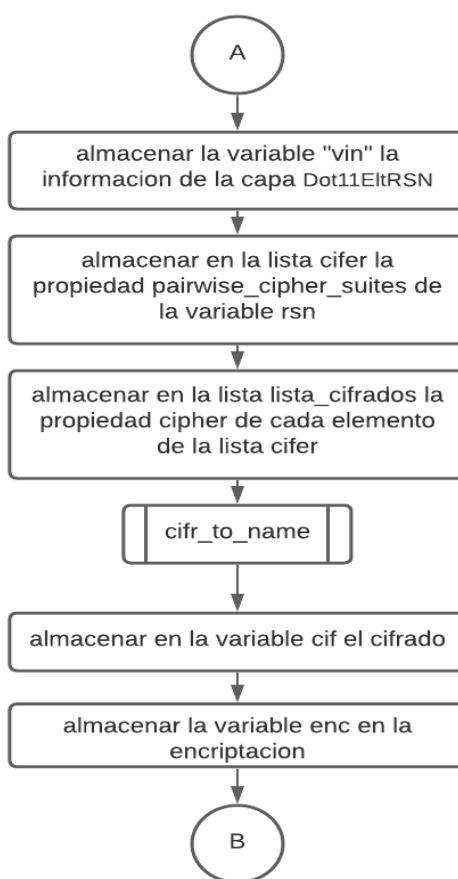




En la Figura 33 se muestra la continuación del diagrama de flujo de la función “inicio\_encryption\_cifrado”, en donde se puede ver la operación a realizar en caso de que el paquete contenga la capa RSN.

### Figura 33

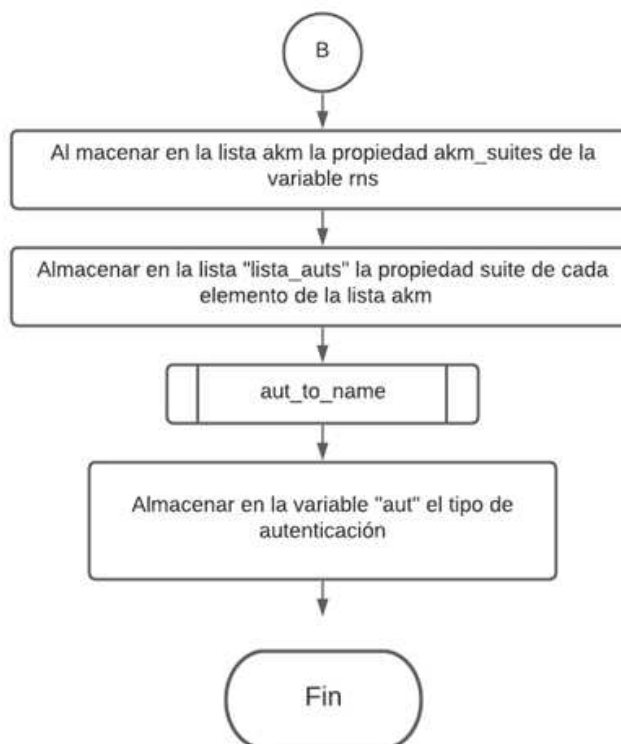
*Diagrama de flujo en caso de que exista la capa Rsn.*



En la Figura 34 se muestra la continuación del diagrama de flujo de la función “inicio\_encryption\_cifrado”, en donde se puede ver la operación a realizar en caso de que el paquete contenga la capa WPA.

### Figura 34

*Diagrama de flujo en caso de que exista la capa Wpa.*



La función “encriptación\_cifrado” consiste en determinar si el paquete capturado contiene las capas Dot11EltRSN o Dot11EltMicrosoftWPA, cualquiera de estas capas retorna un objeto con 2 propiedades importantes:

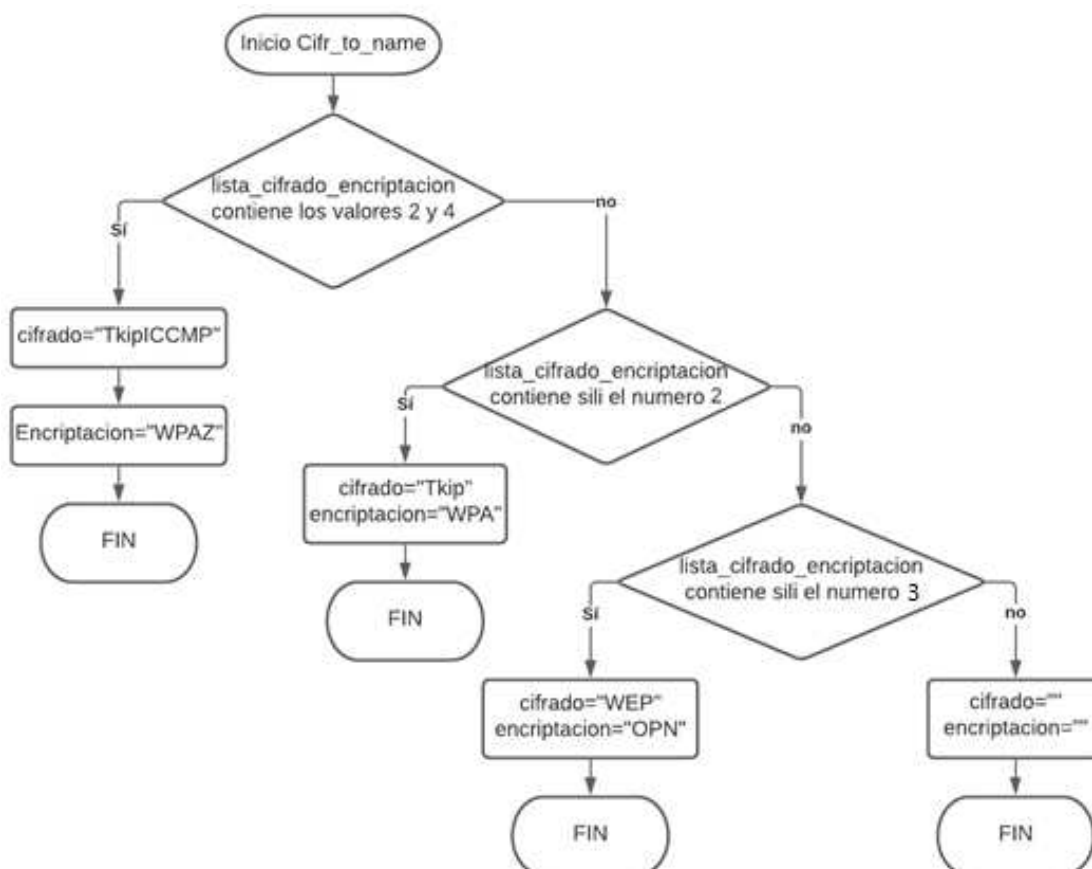
- La primera es “pairwise\_cipher\_suites” mediante la misma se extrae un valor numérico que representa el cifrado y encriptación.
- La segunda es “akm\_suites” mediante la cual se extrae un valor numérico que representa el tipo de autenticación.

Con esta información se llama a las funciones “aut\_to\_name” y “cifr\_to\_name” para obtener los nombres que corresponden a los valores numéricos y se explicara posteriormente.

A continuación en la Figura 35 se muestra el diagrama de flujo de las operaciones realizadas por la función “cifr\_to\_name”.

Figura 35

Diagrama de flujo de la función `cifr_to_name`.



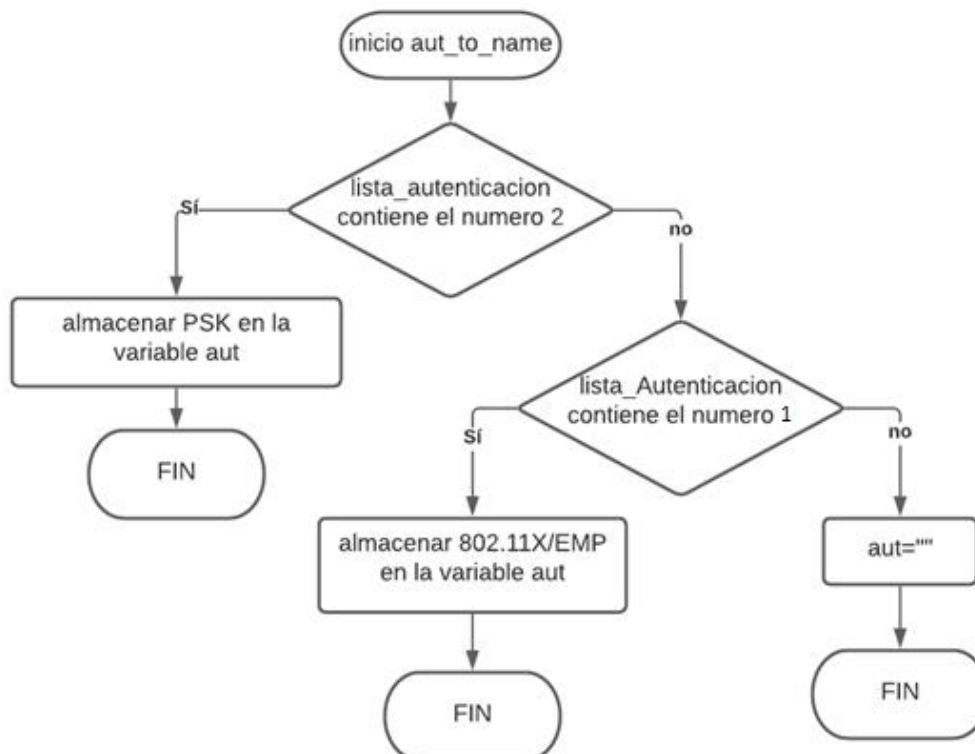
La función “Cifr\_to\_name” permite interpretar el valor numérico obtenido de las capas Dot11EltRSN o Dot11EltMicrosoftWPA donde se pudo comprobar mediante la documentación de scapy que los valores 2 y 4 representan una encriptación de tipo WPA2, si aparece una vez el numero 2 representa WPA y el valor 3 representa el modo abierto “OPN”.

La función “aut\_to\_name” permite interpretar el valor numérico obtenido de las capas Dot11EltRSN o Dot11EltMicrosoftWPA donde se pudo comprobar mediante la documentación de scapy que el valor 2 representa al tipo de autenticación PSK, el valor 1 representa el tipo de autenticación 802.11X basado en el protocolo EAP.

A continuación en la Figura 36 se muestra el diagrama de flujo de las operaciones realizadas por la función `aut_to_name`.

**Figura 36**

*Diagrama de flujo de la función `aut_to_name`.*



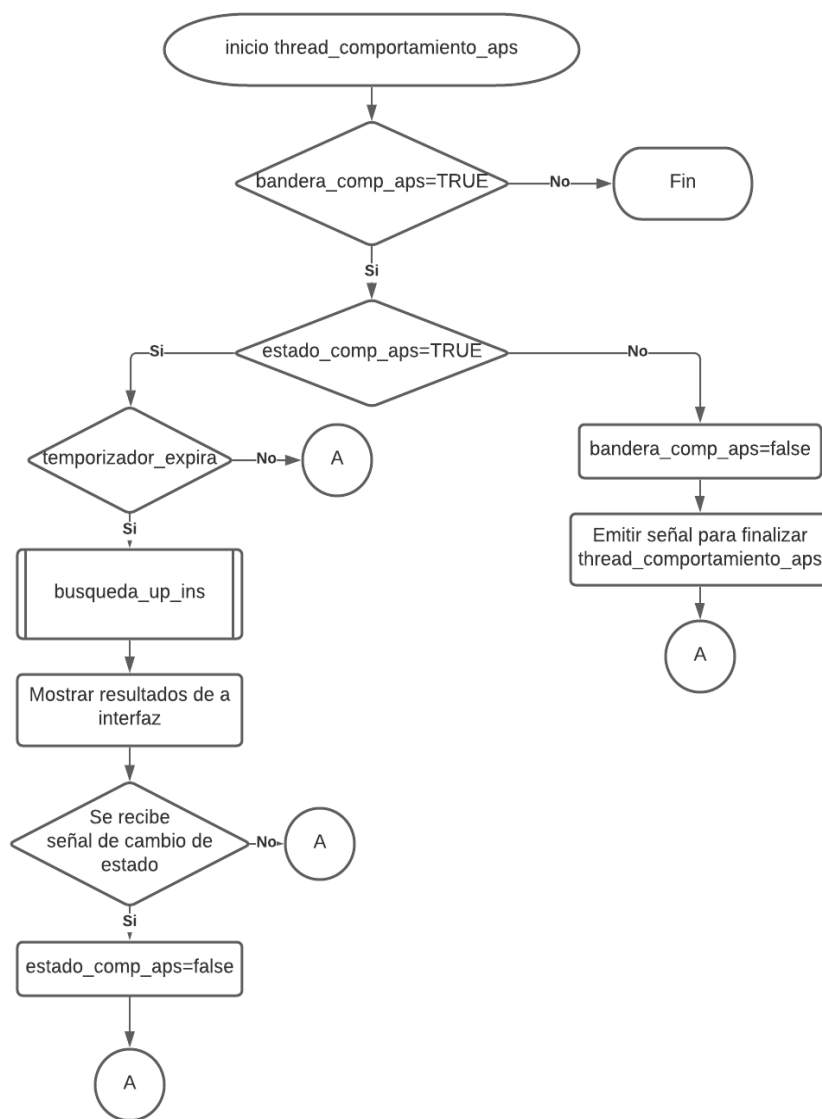
### ***Etapa de Búsqueda y Clasificación***

El hilo “`thread_comportamiento_aps`” lee el estado de las variables “`bandera_comp_ap`” para finalizar con el bucle principal y “`estado_comp_ap`” para finalizar con la ejecución de la función “`búsqueda_up_ins`” y la presentación de los datos en la interfaz. Este hilo cuenta con un temporizador que al expirar llama a la función “`búsqueda_up_ins`” que en resumen clasificara los diferentes subtipos de tramas cursadas por puntos de acceso e identificará al SSID al que pertenece. También se

encarga de mostrar los datos en la pestaña “contador\_tramas\_por\_ap”. En la Figura 37 se muestra el diagrama de flujo de “thread\_comportamiento\_aps”.

**Figura 37**

*Diagrama de flujo de thread\_comportamiento\_aps.*



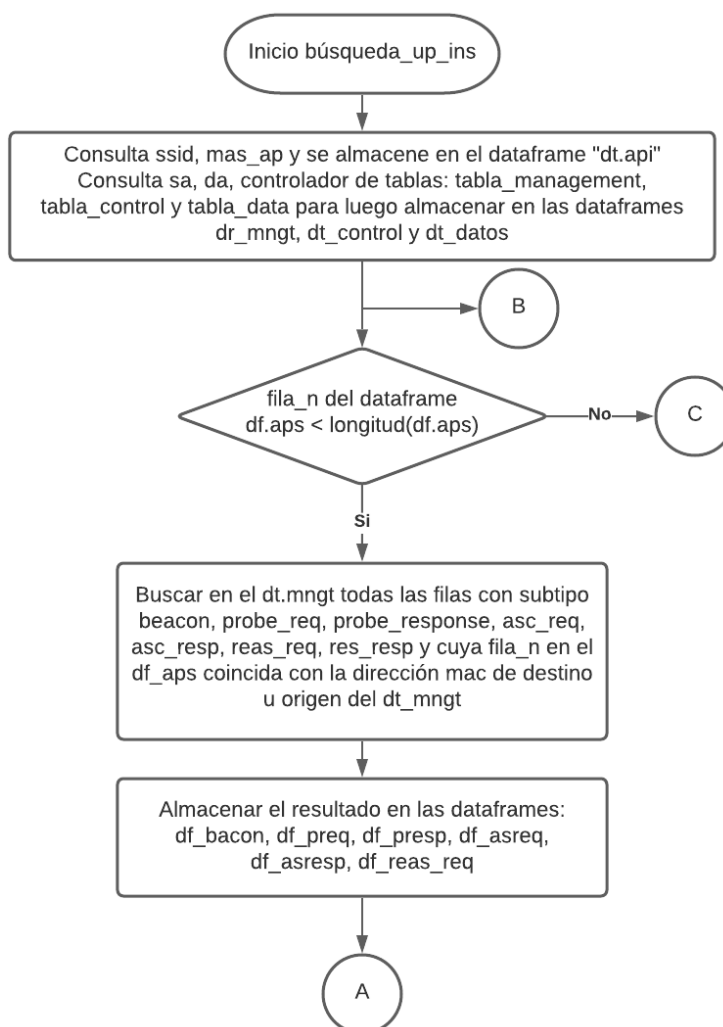
La función “búsqueda\_up\_ins” consiste en extraer en un “dataframe” la información acerca del SSID y la dirección MAC de los puntos de acceso capturados para hacer una búsqueda en las tablas de administración, control y datos para obtener los contadores de cada subtipo de trama encontrada, por cada SSID se sumarán todos

los contadores para posteriormente calcular el porcentaje que representa, por cada búsqueda realizada se comprueba si existen registros en la “tabla\_comp\_aps” para determinar si se actualiza la información o se añade una nueva fila. Gracias al método “iloc” del paquete pandas se facilita la consulta al indicar las condiciones de búsqueda como el subtipo de trama o las direcciones MAC de los puntos de acceso.

A continuación se muestra el diagrama de flujo de “búsqueda\_up\_ins” en la Figura 38.

### Figura 38

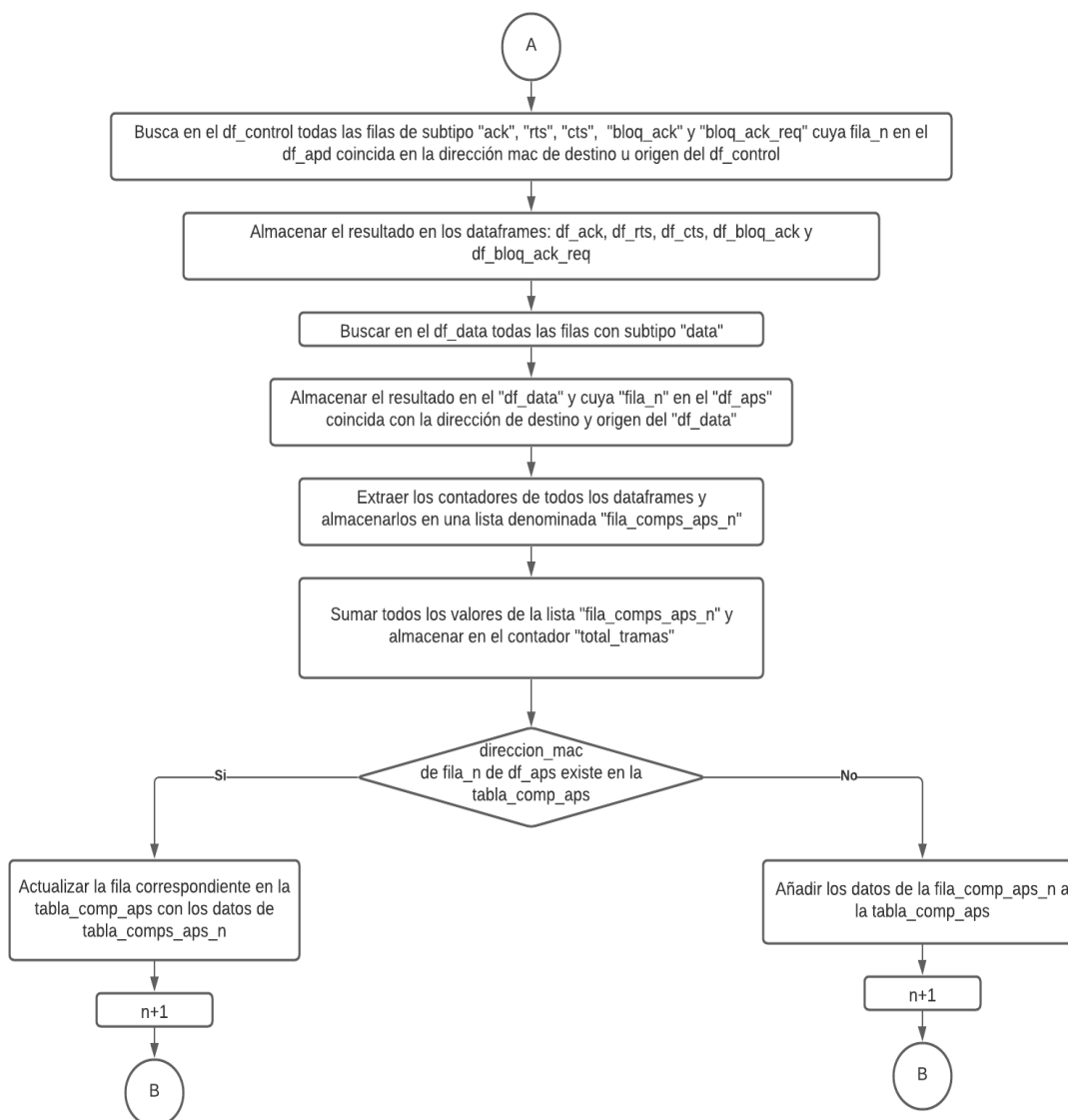
*Diagrama de flujo de la función búsqueda\_up\_ins.*



La Figura 39 muestra la continuación del diagrama de flujo de “búsqueda\_up\_ins”.

**Figura 39**

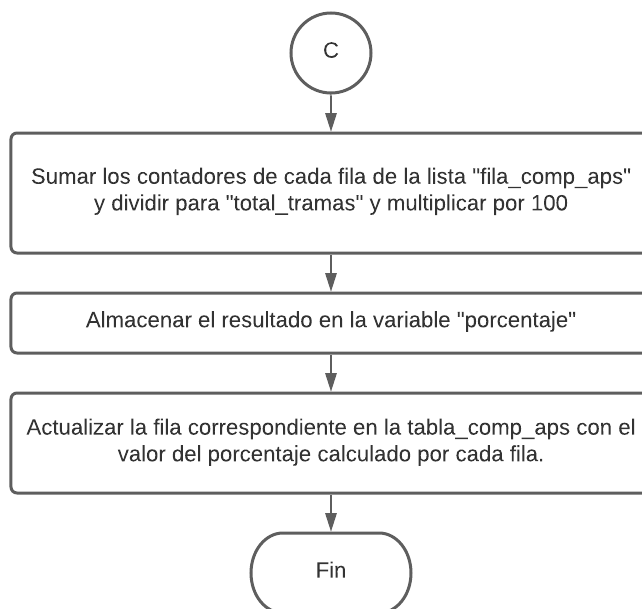
*Continuación del diagrama de flujo de búsqueda\_up\_in.*



A continuación la Figura 40 muestra la condición C que se ve en la Figura 39 en su salida condicional.

**Figura 40**

Condición C de la condicional de búsqueda\_up\_ins.



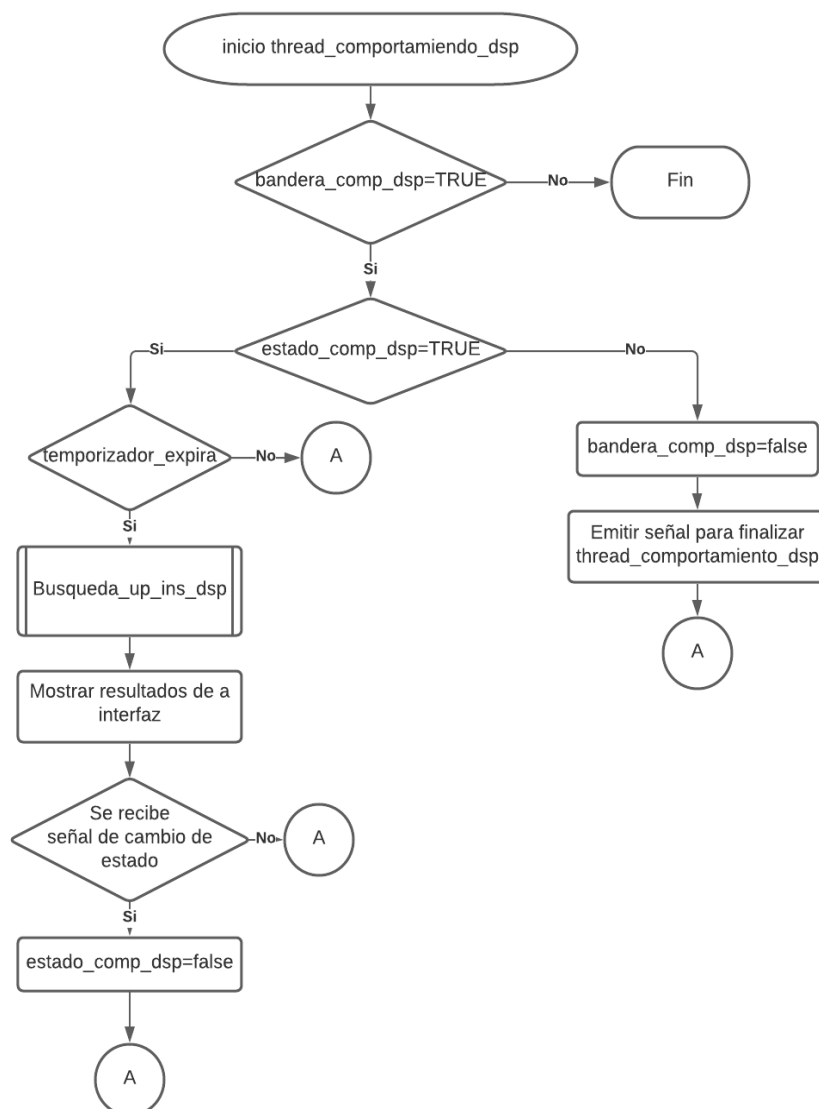
El hilo “thread\_comportamiento\_dsp” lee el estado de las variables “bandera\_comp\_dsp” para finalizar con el bucle principal y “estado\_comp\_dsp” para finalizar con la ejecución de la función “busqueda\_up\_ins\_dsp” y la presentación de los datos en la interfaz. Este hilo cuenta con un temporizador que al expirar llama a la función “busqueda\_up\_ins\_dsp” que en resumen clasificara los diferentes subtipos de tramas cursadas por estaciones e identificara al SSID al que pertenece. También se encarga de mostrar los datos en la pestaña “contador tramas por dispositivo”.

La Figura 41 muestra el diagrama de flujo de la función “thread\_comportamiento\_dsp”.

**Figura 41**

Diagrama de flujo de la función thread\_comportamiento\_dsp.





La función “busqueda\_up\_in\_dsp” consiste en extraer en un “dataframe” la información acerca del SSID y la dirección MAC de las estaciones para hacer una búsqueda en las tablas de administración, control y datos para obtener los contadores de cada subtipo de trama encontrada, por cada SSID se sumarán todos los contadores para posteriormente calcular el porcentaje que representa.

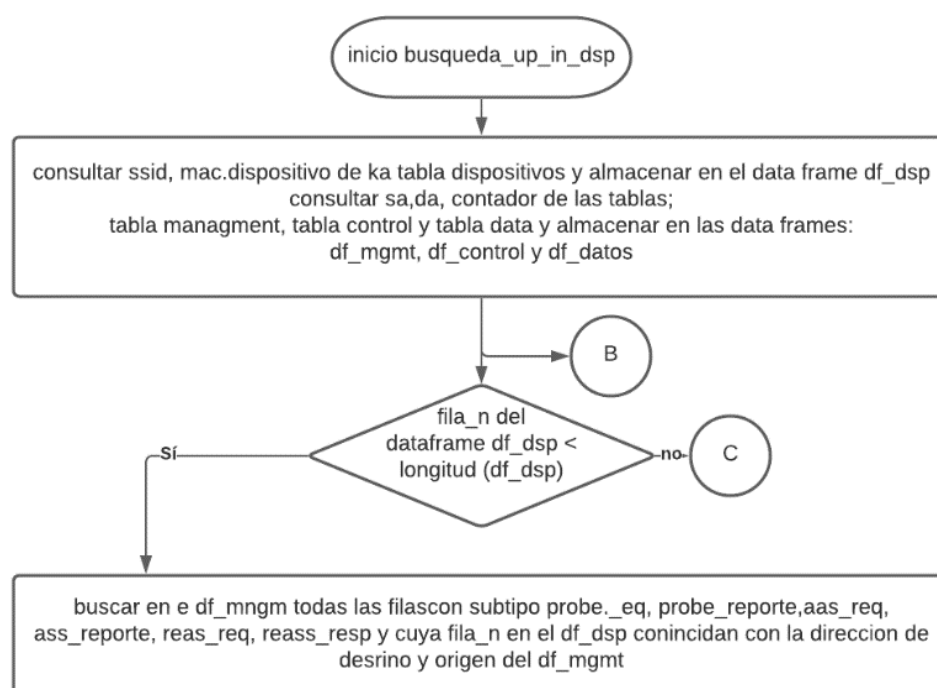
Por cada búsqueda realizada se comprueba si existen registros en la “tabla\_comp\_dsp” para determinar si se actualiza la información o se añade una nueva

fila. Únicamente las tramas “beacon” no se consideran en la búsqueda ya que estas no contienen información acerca de las estaciones.

A continuación en la Figura 42 se muestra el diagrama de flujo de la función “busqueda\_up\_in\_dsp”.

### Figura 42

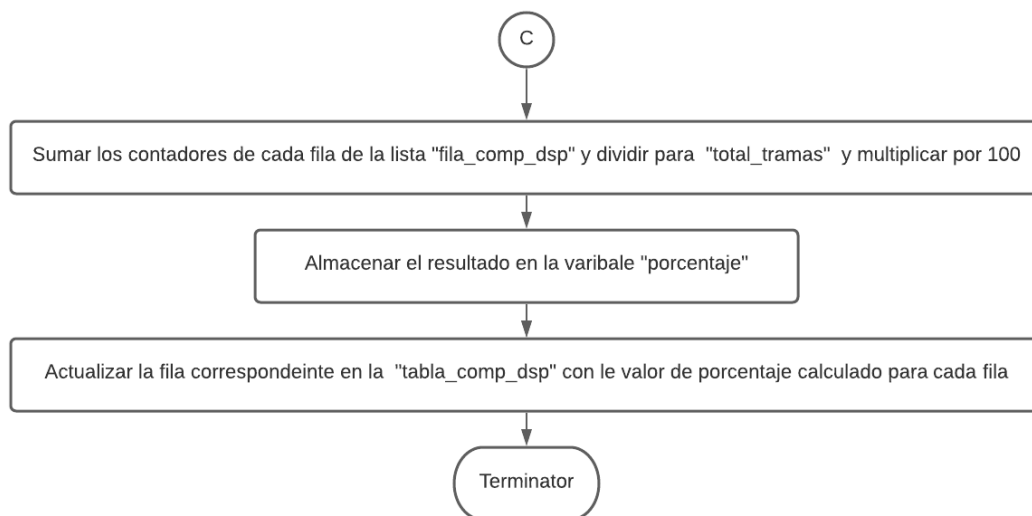
*Diagrama de flujo de busqueda\_up\_in\_dsp.*



Se muestra en la Figura 43 se muestra el proceso derivado de la condicional de la comparación de longitudes de dataframe.

### Figura 43

*Continuación diagrama de flujo busqueda\_up\_disp.*



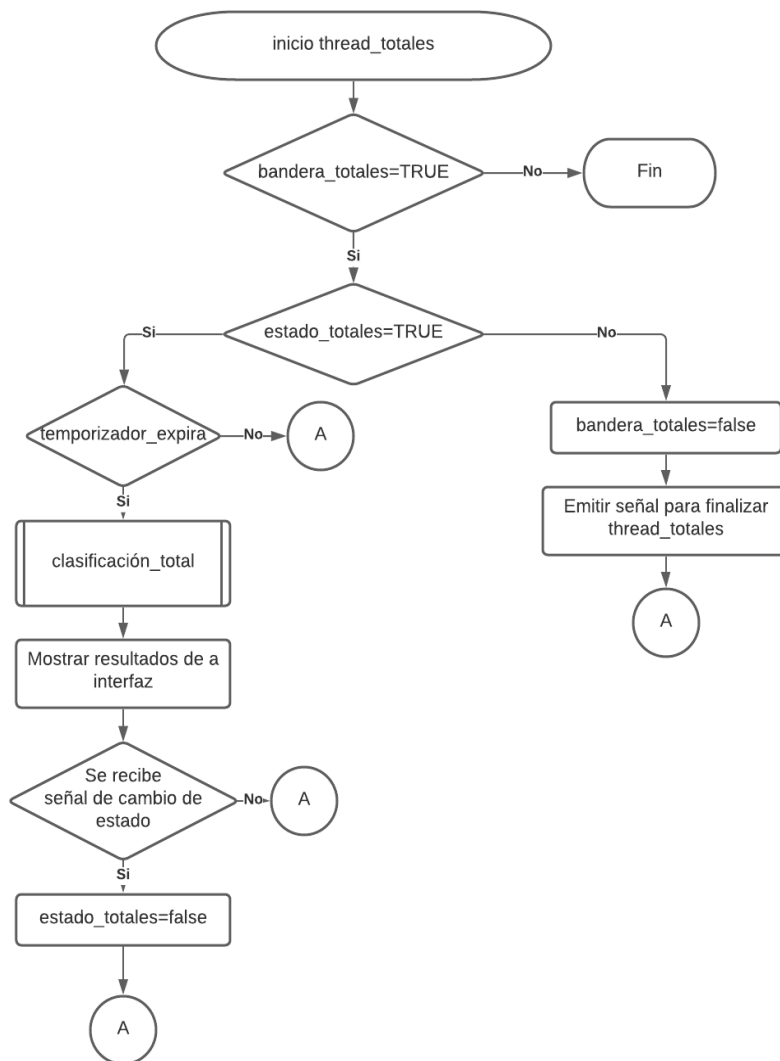
El hilo “thread\_totales” lee el estado de las variables “bandera\_totales” para finalizar con el bucle principal y “estado\_totales” para finalizar con la ejecución de la función “clasificación\_totales” y la presentación de los datos en la interfaz.

Este hilo cuenta con un temporizador que al expirar llama a la función “clasificación\_totales” que en resumen obtiene el total de tramas de administración, control y datos por cada SSID almacenado en la base de datos.

La Figura 44 muestra el diagrama de flujo de la función “thread\_totales”.

#### **Figura 44**

*Diagrama de flujo de la función thread\_totales.*



La función “Clasificaciones\_totales” consiste en extraer en un “dataframe” la información acerca del SSID y la dirección MAC de los puntos de acceso para hacer una búsqueda en la “tabla\_comp\_aps” la misma que contiene contadores para todos los subtipos de tramas analizados en el programa.

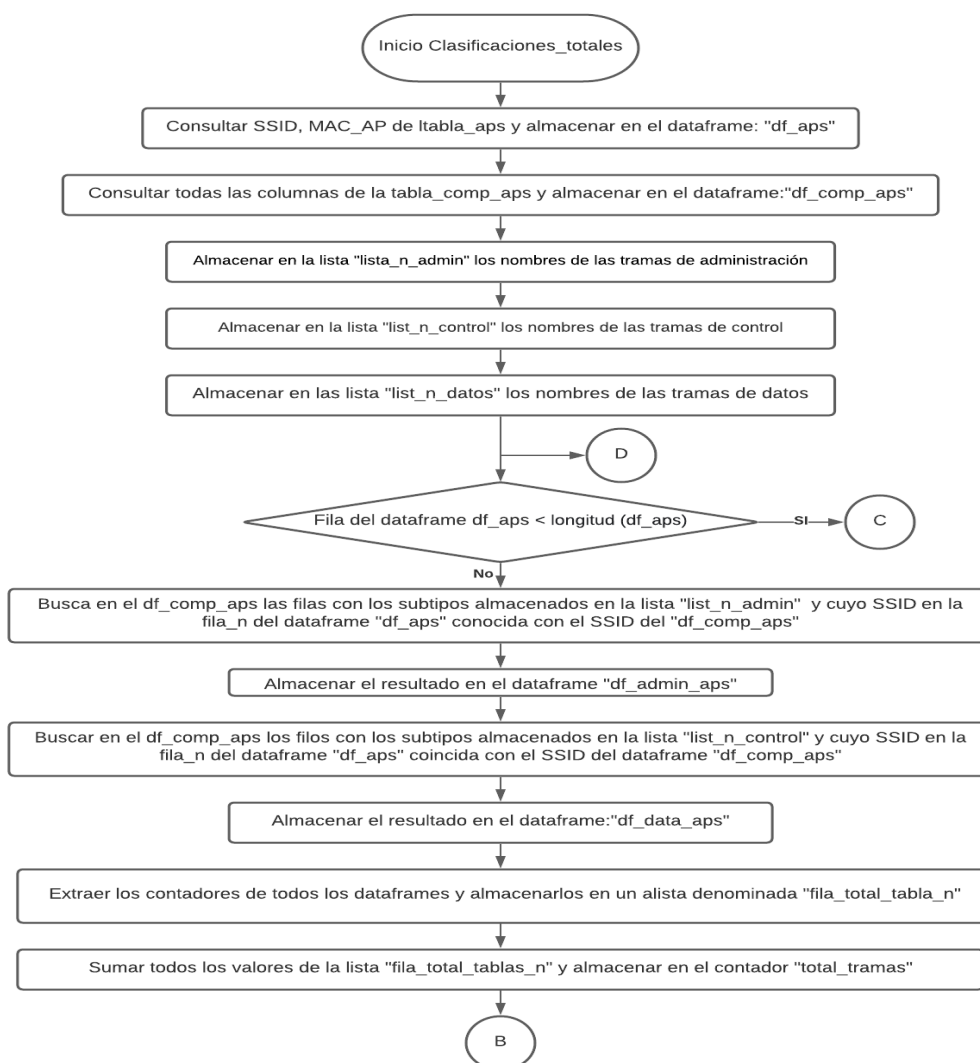
Con ayuda del método “iloc” que poseen todos los “dataframes” se especifican diferentes condiciones para extraer los contadores de tramas de administración, control y datos por cada SSID presentado en la “tabla\_comp\_aps”, también se sumaran contadores por cada fila para posteriormente calcular el porcentaje que representa.

Por cada búsqueda realizada se comprueba si existen registros en “tabla\_totales” para determinar si se actualiza la información o se añade una nueva fila.

A continuación en la Figura 45 se muestra el diagrama de flujo de la función “Clasificaciones\_totales”.

**Figura 45**

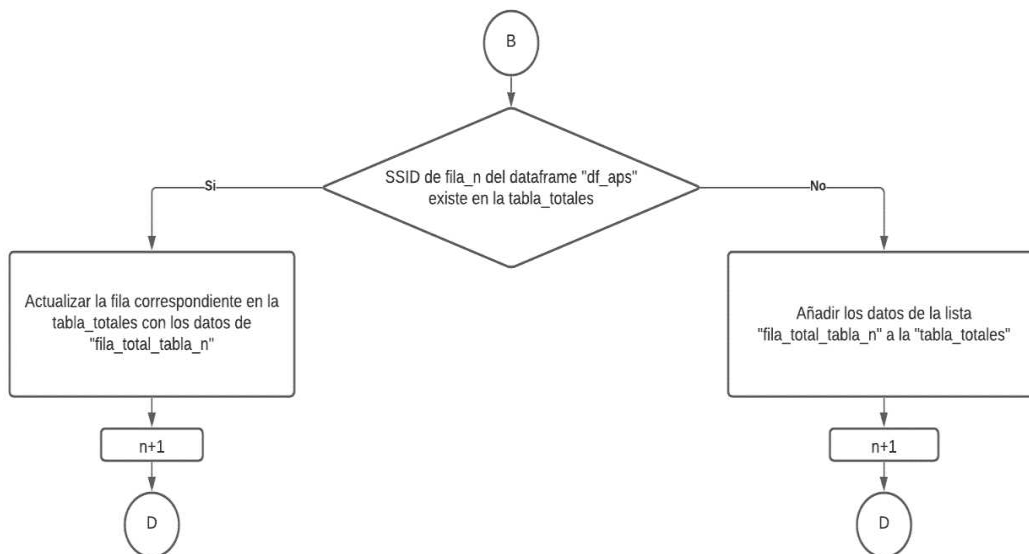
*Diagrama de flujo Clasificaciones\_totales.*



Se muestra la continuación del diagrama de flujo de la función “Clasificaciones\_totales” en la Figura 46.

**Figura 46**

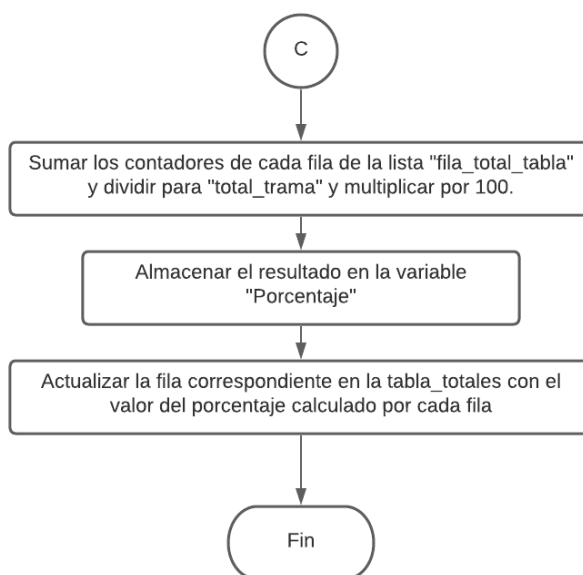
Continuación de la función *Clasificaciones\_totales*.



El proceso derivado de la operación condicional mostrada en la función se muestra en la continuación C y se denota en la Figura 47.

**Figura 47**

Condicional de la función *Clasificaciones\_totales*.



### **Control Panel**

La librería `airpcap.h` tiene información acerca de estructuras de datos y funciones que permiten acceder al driver de Airpcap para seleccionar un canal, hacer conversiones entre frecuencias y canales, configuración WEP, entre otros (Riverbed, 2009).

Para utilizar las funciones que tiene esta librería desde python se utilizó el paquete `ctypes` ya que este permite crear tipos de datos compatibles con el lenguaje C y llamar a funciones contenidas en DLLs (Python) (Rojas, 2019).

La función `cdll` incluida en el paquete `ctypes` permite cargar la librería `airpcap`. Una vez cargada se procede a realizar pruebas de comunicación, es necesario abrir una conexión con el adaptador Airpcap por lo que llama a la función “`AirpcapOpen`” la misma que requiere dos argumentos tipo `string` que representan el nombre del dispositivo y un mensaje de error.

Estos argumentos se crean mediante el método “`create_string_buffer`”, la razón de utilizar este método es que el valor retornado es un objeto cuyo valor en memoria puede ser modificado mediante la propiedad “`raw`”.

El valor retornado al abrir la conexión se denomina “`adapter_handle`” debe ser diferente de cero y se utilizará para seleccionar un canal. En esta etapa se pudo comprobar que la versión 3 de python siempre retorna un valor igual a cero por lo que fue necesario utilizar la versión 2.7.

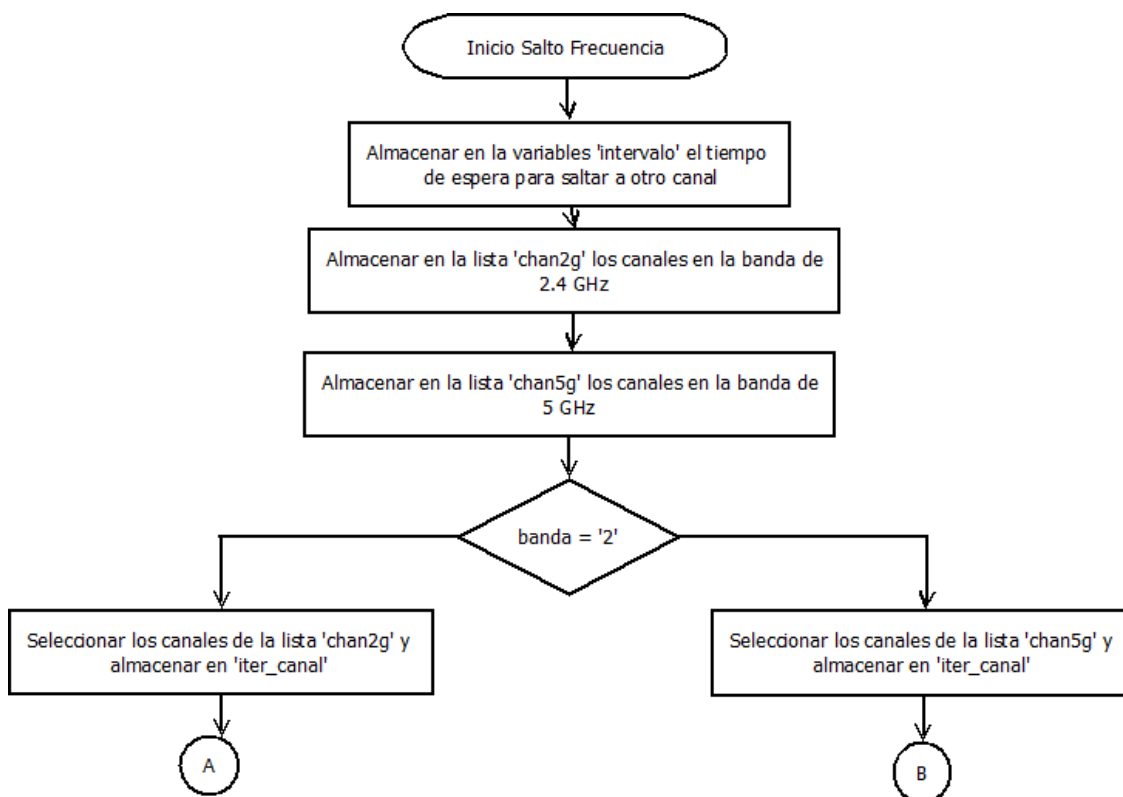
Para seleccionar canales durante el salto de frecuencia se usa la función “`AirpcapSetDeviceChannel`” la cual requiere dos argumentos que son “`adapter_handle`” y el número de canal, el valor retornado será igual a 1 si se logró especificar el canal deseado.

### Salto Frecuencia

La Figura 48 muestra el diagrama de flujo de la función “Salto Frecuencia”, donde se detalla la selección o salto de canales en la banda de frecuencia 2.4 GHz.

**Figura 48**

*Diagrama de flujo de la función Salto Frecuencia.*

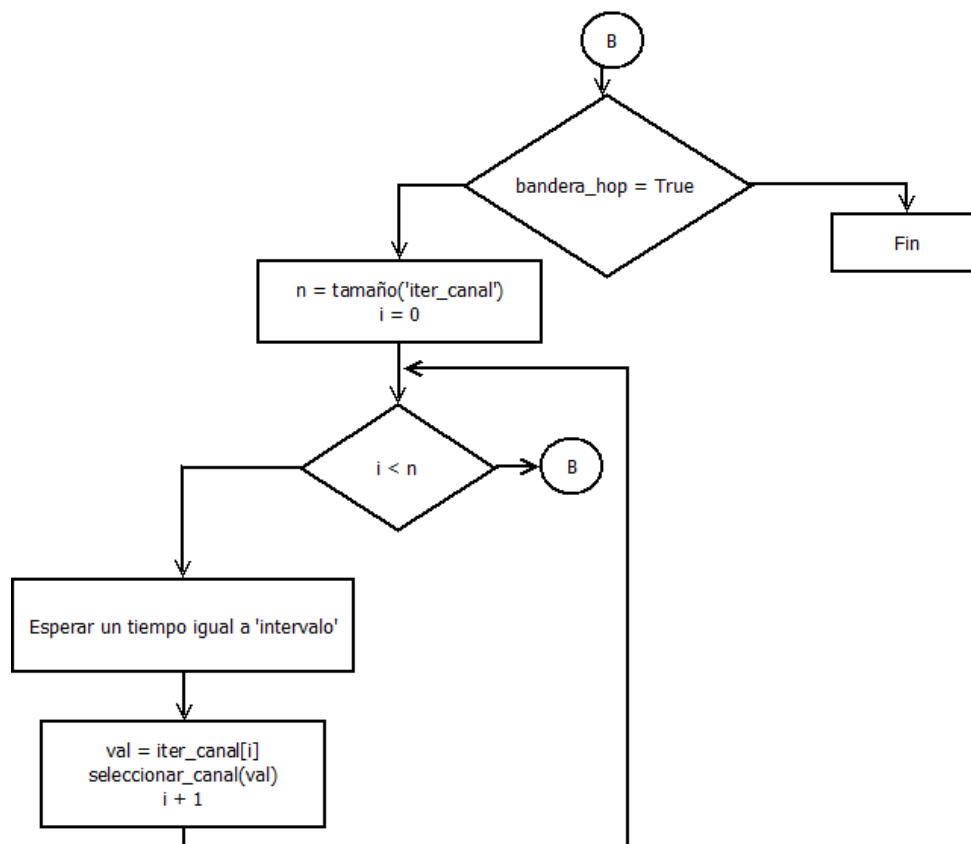


Para hacer saltos de frecuencia se necesita que el usuario especifique el “intervalo” que es el tiempo que tarda en hacer un nuevo salto en milisegundos, también es necesario seleccionar la banda para crear una lista con los canales de 2.4GHz o 5 GHz. Una vez especificada esta información se harán los saltos con ayuda de la función “AirpcapSetDeviceChannel” para seleccionar el canal. En la Figura 49 se muestra la continuación de la función Salto Frecuencia.

**Figura 49**

*Continuación de la función Salto Frecuencia.*

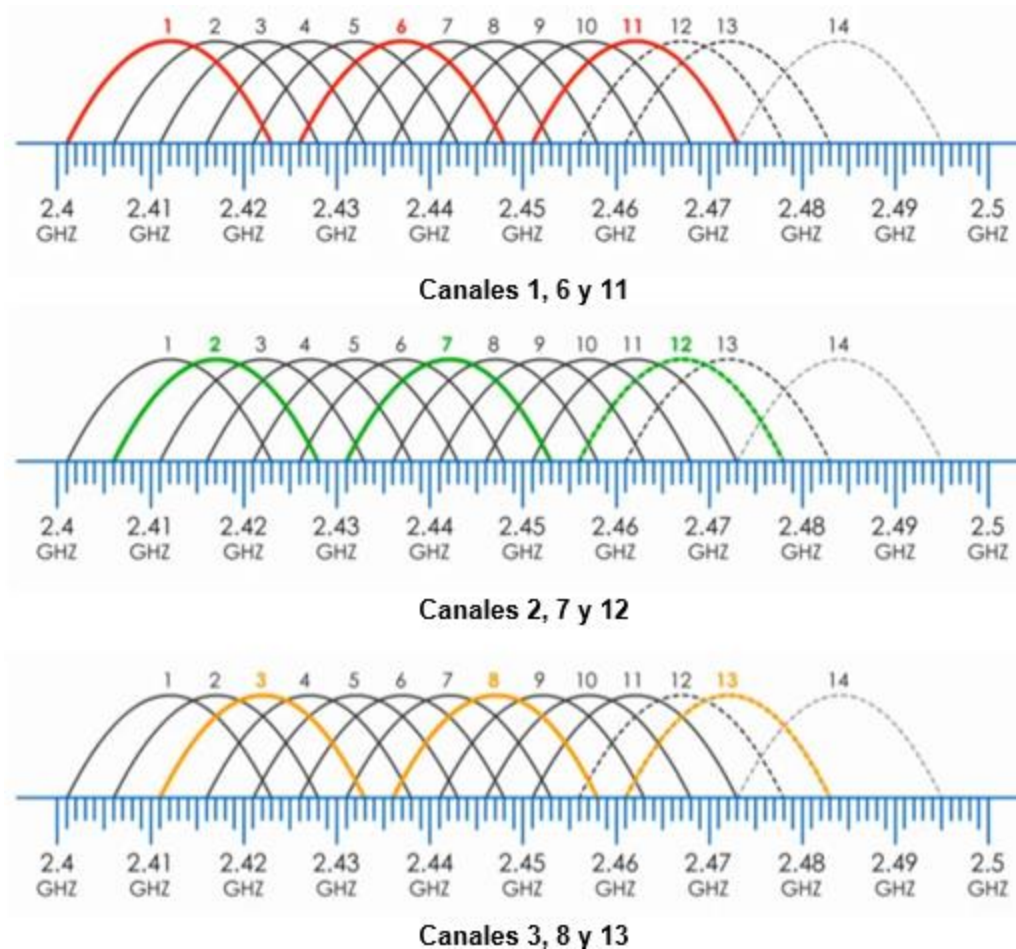




Es importante destacar que en la banda de 2.4 GHz existe solapamiento entre canales adyacentes por lo que la lista 'chan2g' contiene los siguientes valores: 1, 6, 11, 2, 7, 12, 3, 8, 13; estos valores representan los canales en los cuales hará el salto de frecuencia para evitar interferencias como se muestra en la Figura 50 (Geier, 2015).

### Figura 50

*Solapamiento de canales en la frecuencia de 2.4 GHz.*

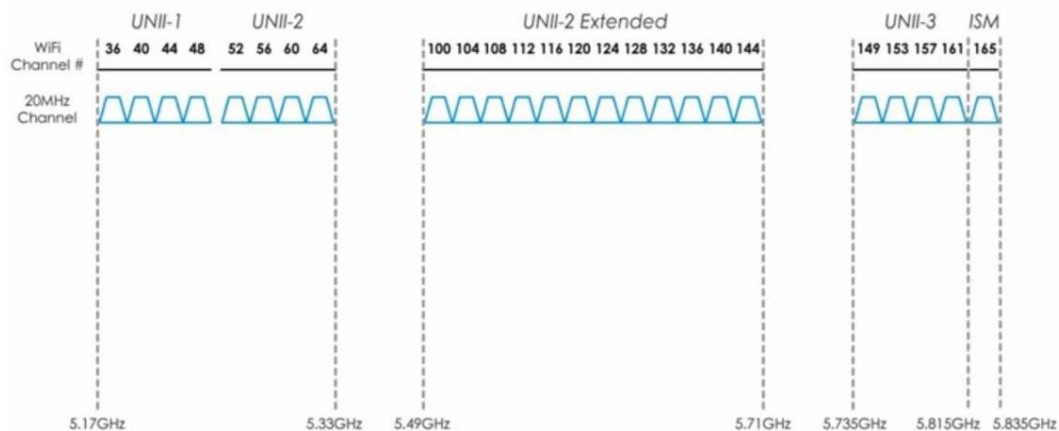


*Nota.* Tomado de *Como configurar los canales wifi para un mejor rendimiento de la red*, por Wordpress., 2015, Wordpress (<https://jmvinanza.wordpress.com/2015/11/05/cmo-configurar-los-canales-wifi-para-un-mejor-rendimiento-de-la-red/>).

En la Figura 51 se observa que en la banda de 5 GHz no se presenta este problema por lo que se creó una lista con canales de la banda UNII 1, 2, 3 e ISM en orden ascendente (Geier, 2015).

### **Figura 51**

*Solapamiento de canales en la frecuencia de 5 GHz.*



*Nota.* Tomado de *Como configurar los canales wifi para un mejor rendimiento de la red*, por Wordpress., 2015, Wordpress (<https://jmvinazza.wordpress.com/2015/11/05/cmo-configurar-los-canales-wifi-para-un-mejor-rendimiento-de-la-red/>).

### **Canal Fijo**

Para la selección de un canal fijo el usuario es quien selecciona un canal de una lista desplegable y también un ancho de banda de 20MHz o 40 MHz. En esta etapa se necesita dos funciones de la librería de airpcap. La primera es “AirpcapConvertChannelToFrequency” que permite convertir un canal a frecuencia en MHz y este valor es almacenado en una variable para utilizarse en la segunda función denominada “AirpcapSetDeviceChannelEx”. Esta función permite seleccionar un canal principal y un canal de secundario de modo que se pueda formar un canal de 40MHz, en caso de necesitar un canal de 20 MHz que es la opción por defecto no se selecciona un canal secundario.

En esta etapa se pudo revisar los comentarios disponibles en la librería airpcap.h. Donde se muestran 2 posibles opciones de selección de canal principal y secundario.

Al seleccionar -1 el canal secundario será menor al canal principal, si el usuario selecciona +1 el canal secundario será mayor al canal principal, cuando se elige estas

opciones automáticamente la función “AircapSetDeviceChannelEx” seleccionara un canal secundario con una diferencia de 4 canales para evitar solapamientos por lo que

La última consideración fue condicionar cuando seleccionar 1 y -1 en la banda de 2.4 GHz o 5GHz.

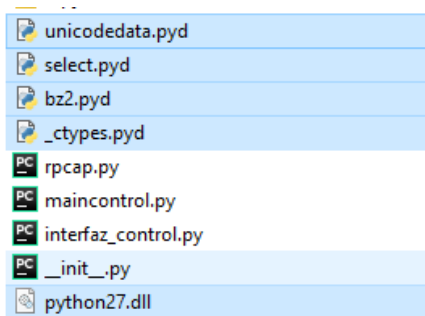
En la banda de 2.4 GHz se seleccionara +1 cuando el usuario seleccione canales entre 1 a 9, mientras que -1 cuando se seleccione canales del 10 al 14. En la banda de 5GHz se seleccionara +1 en todos los canales con excepción del canal 165 de esta manera evitamos sobrepasar la banda de frecuencias disponible.

### **Compatibilidad con Python 3**

Debido a que se creó el script para seleccionar canal y hacer salto de frecuencia en Python 2.7 se crea un ejecutable de este programa mediante el módulo py2exe el cual genera varios archivos que deben estar en el mismo directorio desde donde se inicia el ejecutable. En la Figura 52 podemos ver los archivos necesarios para iniciar el ejecutable control\_c.exe.

#### **Figura 52**

*Archivos para el ejecutable de control\_c.*



Una vez creado este ejecutable se puede iniciarlo con la opción -h para ver las opciones disponibles como se observa en la Figura 53.

#### **Figura 53**

*Archivos disponibles en control\_c.*

```
Options:
-h, --help          show this help message and exit
-a, --airp          identificador de airpcap
-b, --banda         seleccionar banda de frecuencia
-p, --paso          seleccionar valor de salto entre canales
-i, --intervalo    seleccionar intervalo de tiempo para cambio de canal
-c, --canal        seleccionar un solo canal
-e, --extension     seleccionar un canal de extension
```

Como se observa en la Figura 53 se requiere especificar el identificador de la tarjeta airpcap el cual inicia con “\\.\airpcapxx”, “xx” representa un número único por cada adaptador conectado.

También es necesario indicar la banda de frecuencia que puede ser ‘2’ o ‘5’ que corresponde a 2.4GHz o 5GHz. EL intervalo que indica el tiempo que se debe esperar antes de hacer un nuevo salto.

En caso de seleccionar un solo canal se debe seleccionar el identificador de la tarjeta el canal y la extensión. La opción extensión puede tomar 3 valores diferentes que son los siguientes: ‘1’ representa +1 es decir que se selecciona un canal principal y un canal secundario mayor al principal, ‘2’ representa -1 y selecciona un canal principal y un canal secundario menor al principal y ‘3’ representa 0 que es el valor por defecto y que solo selecciona un canal principal. Por lo tanto la opción 1 o -1 representa un ancho de banda de 40 MHz y 0 representa 20 MHz.

## **Interfaz Gráfica del Aplicativo**

### ***Programa Pantalla Principal***

En la Figura 54 se puede observar en el panel izquierdo los botones para controlar la interfaz, inicialmente se encuentran bloqueados hasta que se presione el botón de abrir conexión con la base de datos, luego se necesita seleccionar una interfaz mediante la lista desplegable al seleccionar la interfaz de desbloqueará el panel de control de la interfaz la cual permite al usuario seleccionar el ancho de banda, la frecuencia de captura, el modo de trabajo ya sea este salto en frecuencia o un canal fijo

de trabajo; posteriormente se puede iniciar la captura. Los datos se irán mostrando en las tablas del panel derecho, mientras se captura los datos los demás botones del panel izquierdo se bloquean hasta que se presione el botón de parar.

## Figura 54

*Pantalla principal.*

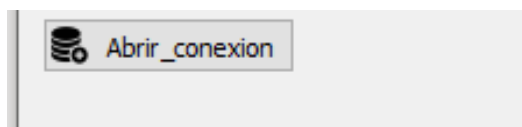


### **Botón de Conexión a la Base de Datos**

En la Figura 55 se observa el botón de abrir conexión el cual ejecuta una función que verificara que las credenciales almacenadas en el archivo my.ini sean las correctas caso contrario se muestra un mensaje de alerta indicando que no es posible conectarse con la base de datos y bloqueara los demás botones del panel de control.

## Figura 55

*Botón de conexión con la base de datos.*



## Base de Datos

En la Figura 56 se creó una base de datos llamada Windows Sniffer donde se encuentran las tablas en las cuales se almacena toda la información respecto a los contadores de los paquetes capturados, así como la clasificación de estos dependiendo del tipo de trama. Los datos que se almacenan en las columnas “contador” son de tipo entero, las columnas “Porcentaje” son de tipo flotante y el resto de columnas son de tipo Varchar.

**Figura 56**

*Base de datos Windows Sniffer.*

Tabla	Acción	Filas	Tipo	Cotejamiento	Tamaño	Residuo a depurar
<input type="checkbox"/> tabla_aps	★ Examinar Estructura Buscar Insertar Vaciar Eliminar	3	InnoDB	utf8mb4_general_ci	16.0 KB	-
<input type="checkbox"/> tabla_comp_aps	★ Examinar Estructura Buscar Insertar Vaciar Eliminar	3	InnoDB	utf8mb4_general_ci	16.0 KB	-
<input type="checkbox"/> tabla_comp_dsp	★ Examinar Estructura Buscar Insertar Vaciar Eliminar	0	InnoDB	utf8mb4_general_ci	16.0 KB	-
<input type="checkbox"/> tabla_control	★ Examinar Estructura Buscar Insertar Vaciar Eliminar	15	InnoDB	utf8mb4_general_ci	16.0 KB	-
<input type="checkbox"/> tabla_data	★ Examinar Estructura Buscar Insertar Vaciar Eliminar	0	InnoDB	utf8mb4_general_ci	16.0 KB	-
<input type="checkbox"/> tabla_managment	★ Examinar Estructura Buscar Insertar Vaciar Eliminar	17	InnoDB	utf8mb4_general_ci	16.0 KB	-
<input type="checkbox"/> tabla_totales	★ Examinar Estructura Buscar Insertar Vaciar Eliminar	3	InnoDB	utf8mb4_general_ci	16.0 KB	-
7 tablas	Número de filas	41	InnoDB	utf8mb4_general_ci	112.0 KB	0 B

## Panel de Control Principal, de canal, ancho de banda y salto de Frecuencia.

### Panel de Control Principal

El botón verde permite iniciar los hilos de captura, procesamiento, clasificación de puntos de acceso y dispositivos, contadores de tramas cursadas por puntos de acceso y dispositivos y también para mostrar los datos en la interfaz gráfica.

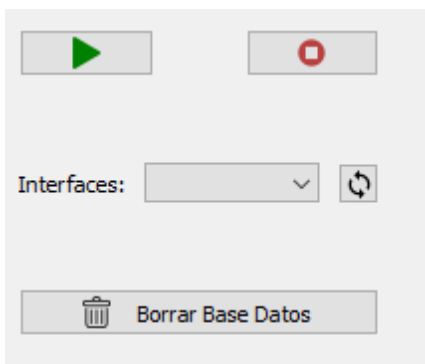
- El botón rojo permite llamar a al método quit() para terminar de manera segura con todos los hilos iniciados.
- La lista junto a la etiqueta “interfaces” permite seleccionar tarjetas de red que se encuentren en modo monitor.
- EL botón borrar base datos permite eliminar los datos de las tablas y en la interfaz gráfica.

- El botón actualizar permite llamar a una función que buscare interfaces en modo monitor mediante un comando de la herramienta tshark.

La Figura 57 muestra el diseño del panel de control de la interfaz.

### Figura 57

*Panel de control de la interfaz.*



### **Control Panel de Canal, Ancho de Banda y Salto de Frecuencia**

Se tienen dos opciones de selección en el panel que son:

- En la sección “Selección Canal fijo” se puede seleccionar el canal en el cual la tarjeta realizará la captura de paquetes, esta selección puede ser en 2,4 GHz. y 5 GHz; adicionalmente en esta sección se debe escoger el ancho de banda al cual trabajará la tarjeta seleccionada.
- En la sección “Salto en frecuencia” se puede seleccionar la frecuencia en la que la tarjeta realizará los saltos para la captura de paquetes, así como también el tiempo en milisegundos, esta selección puede ser en 2,4 GHz. y 5 GHz.

En la Figura 58 se muestra el Control Panel de la tarjeta y su diseño.



**Figura 58**

*Control panel de la tarjeta.*



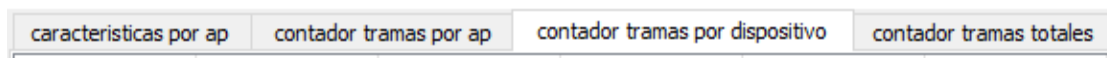
### ***Tablas de Clasificación de las Tramas Capturadas***

En la Figura 59 se puede observar las siguientes tablas:

- Características por AP: Esta tabla muestra características de puntos de acceso como tipo de encriptación, cifrado, autenticación, su dirección MAC y la red a la que pertenece.
- Contador de tramas por AP: Esta tabla muestra contadores de subtipos de tramas de administración, control y datos cursados por cada punto de acceso, también representa el porcentaje de tramas por ssid.
- Contador de tramas por dispositivo: Esta tabla muestra contadores de subtipos de tramas de administración, control y datos cursados por cada estación, también representa el porcentaje de tramas por cada dispositivo perteneciente a una red.
- Contador de tramas totales: Esta tabla calcula el total de tramas de tipo administración, control y datos por cada ssid y también muestra el porcentaje de paquetes que representa cada red.

## Figura 59

*Tablas de clasificación de las tramas capturadas.*

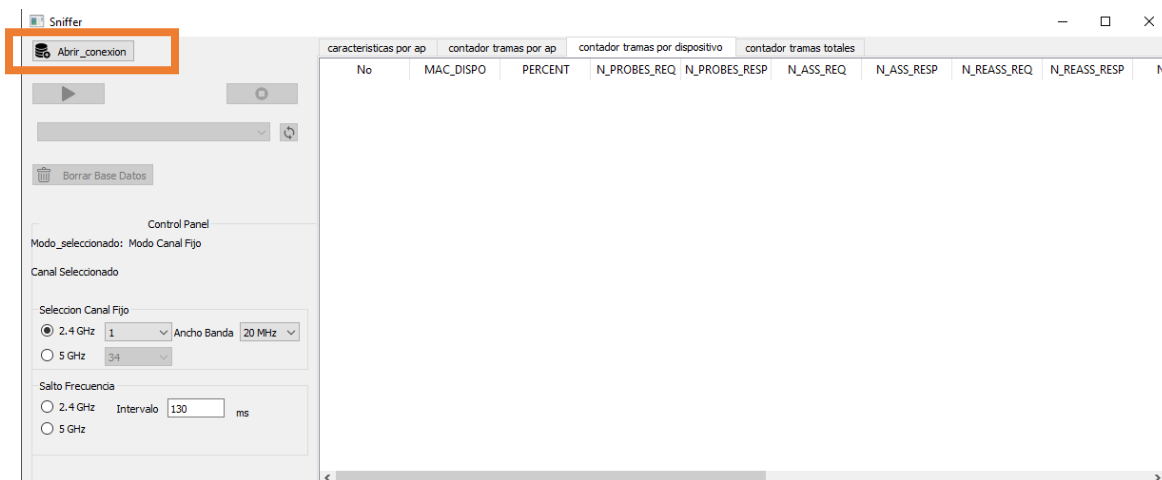


## Detalle de Funcionamiento del Dispositivo

El aplicativo desarrollado en Python permite capturar y caracterizar tramas 802.11 en Windows. Para iniciar el programa de debe Abrir la base de datos pulsando el botón que se encuentra en la parte superior izquierda, en la Figura 60 se puede observar que el programa bloquea todas las opciones de selección y ejecución del programa debido a que no se pudo enlazar a la base de datos, en el caso de existir problemas de conexión con la misma, el programa enviará una alerta al usuario la cual le indicará que no está conectado a la base de datos.

## Figura 60

*Ventana principal sin conexión a la base de datos.*

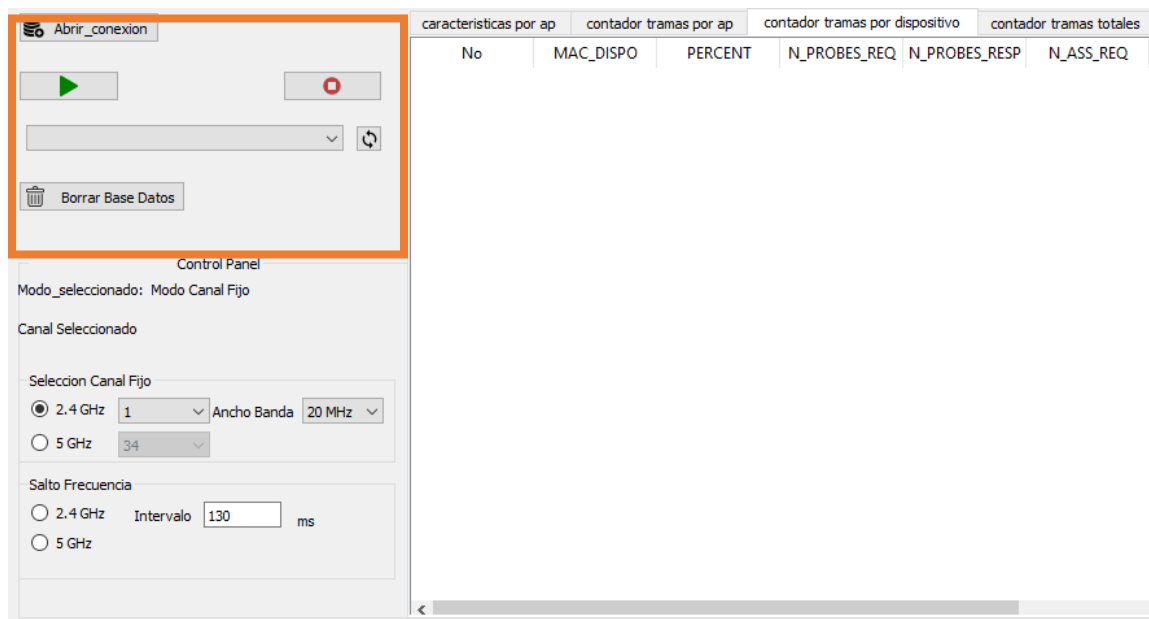


Luego de establecer la conexión con la base de datos, el programa activará los botones del panel de control principal. En la Figura 61 se muestra que el programa desarrollado activa los botones de inicio(verde), parar(rojo), selección de la tarjeta de

red, botón para actualizar interfaces conectadas y el botón para eliminar los datos almacenados en la base de datos.

### Figura 61

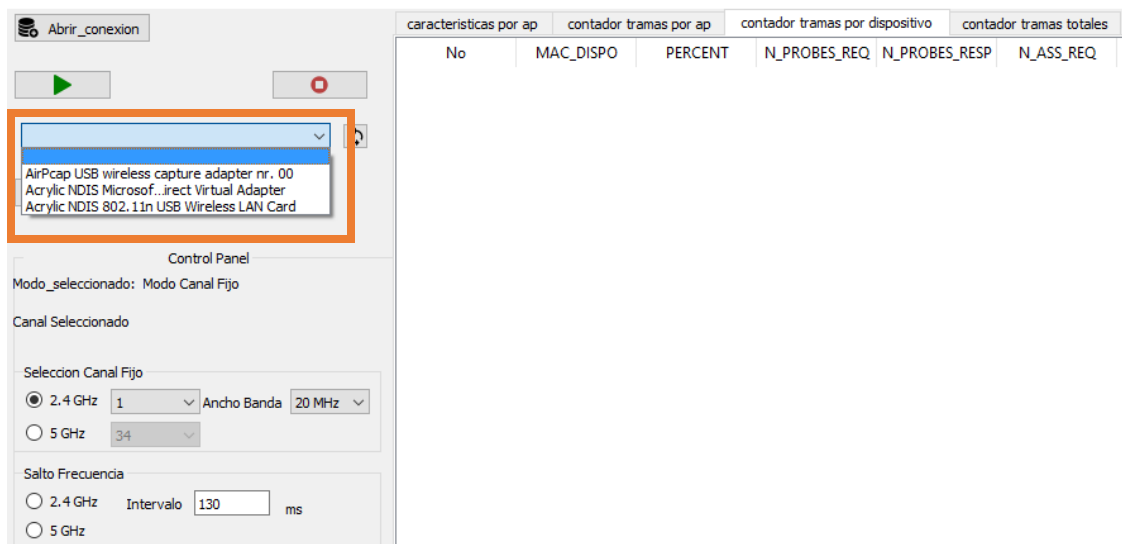
*Activación del panel de control principal para la selección de la interfaz.*



Para seleccionar el adaptador de red inalámbrico se debe presionar sobre el rectángulo que se encuentra debajo de los botones de inicio(verde) y parar(rojo), aquí el programa mostrará las interfaces en modo monitor compatibles para realizar la captura de paquetes. En la Figura 62 se muestra como se despliegan diferentes adaptadores de red en modo monitor.

### Figura 62

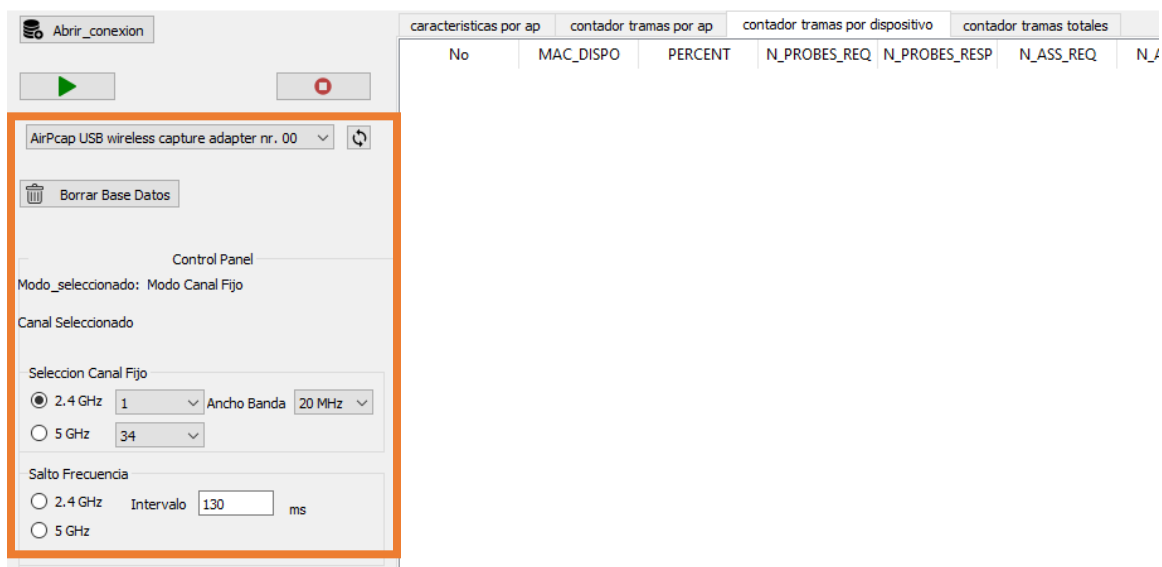
*Despliegue de los adaptadores de red.*



Al seleccionar la tarjeta de red inalámbrica con la cual se va realizar la captura de los paquetes, el “Control Panel” dependiendo de la compatibilidad de la tarjeta con el controlador de acrylic activará o desactivará las diferentes opciones de configuración de la tarjeta de red seleccionada. En la Figura 63 se visualiza la activación del “Control Panel” al seleccionar la tarjeta “AirPcap Nx”.

### Figura 63

*Selección de la tarjeta de red y activación del Control Panel.*



El programa luego de iniciar la captura de paquetes permitirá que usuario visualice cuatro tablas. En la Figura 64 se muestra la tabla “Características por ap” la cual permite visualizar el nombre de los SSID, su dirección MAC, encriptación, cifrado, autenticación, potencia(dBm), canal y frecuencia.

**Figura 64**

*Sección de Características por ap.*

características por ap		contador tramas por ap	contador tramas por dispositivo	contador tramas totales				
	SSID	MAC_AP	ENCRIPCIÓN	CIFRADO	AUTENTICACION	POTENCIA(dBm)	CANAL	FRECUENCIA
1	CELERITY_BRAVO	44:65:7f:8e:fa:00	CCMP	WPA2	PSK	-49	2462	11
2	Claro_FERNADOO...	30:93:bc:eb:dc:2e	TKIP CCMP	WPA2	PSK	-77	2462	11
3	Claro_VALENCIA0...	5c:b1:3e:5b:8b:5e	TKIP CCMP	WPA2	PSK	-78	2462	11
4	Claro_RAMOS0007...	10:33:bf:7e:f2:22	CCMP	WPA2	PSK	-81	2462	11
5	Claro_NELSONIM...	a4:15:88:eb:02:50	TKIP CCMP	WPA2	PSK	-80	2462	11
6	Claro_VELASTEGUI...	ac:ec:80:96:b8:60	TKIP CCMP	WPA2	PSK	-80	2462	11
7	Omn_i_lite556540	34:21:09:65:65:49	TKIP CCMP	WPA2	PSK	-81	2462	11
8	SOFIA_CNT	bc:c0:0f:95:8b:18	TKIP CCMP	WPA2	PSK	-57	2412	1
9	NETLIFE-...	3c:37:86:74:80:6c	TKIP CCMP	WPA2	PSK	-68	2412	1
10	NETLIFE-Carrillo	94:04:9c:67:32:80	TKIP CCMP	WPA2	PSK	-70	2412	1

En la Figura 65 se muestra la tabla “Contador de tramas por ap” la cual permite visualizar el detalle de cada uno de los subtipos de tramas como son: Beacons, Probe Request, Probe Response, Association Request, Association Response, Reas. Request, Reas. Response, Authentication, DE authentication, Acknowledgement, Request to Send, Clear to Send y Data. Estos datos se detallan de cada uno de los Access Point encontrados.

**Figura 65**

*Sección Contador de tramas ap.*

	SSID	BSSID	PERCENT	N_BEACONS	N_PROBES_REQ	N_PROBES_RESP	N_ASS_REQ	N_ASS_RESP	N_REASS_REQ
1	CELERITY_BRA...	44:65:7f:8e:fa:00	58.9693	1033	0	81	0	0	0
2	Claro_FERNAD...	30:93:bc:eb:dc:...	2.14734	60	0	3	0	0	0
3	Claro_VALENC...	5c:b1:3e:5b:8b:...	0.99108	27	0	2	0	0	0
4	Claro_RAMOS...	10:33:bf:7e:f2:22	0.396432	9	0	3	0	0	0
5	Claro_NELSON...	a4:15:88:eb:02:50	0.16518	4	0	0	0	0	0
6	Claro_VELASTE...	ac:ec:80:96:b8:60	0.066072	2	0	0	0	0	0
7	Omni_lite656540	34:21:09:65:65:49	0.627684	5	0	0	0	0	0
8	SOFIA_CNT	bc:c0:0f:95:8b:18	35.0512	452	0	11	0	0	0
9	NETLIFE-...	3c:37:86:74:80:6c	1.35448	39	0	1	0	0	0
10	NETLIFE-Carrillo	94:04:9c:67:32:80	0.231252	6	0	0	0	0	0

En la Figura 66 se muestra la tabla “Contador de tramas por dispositivos” la cual permite visualizar el detalle de cada uno de los subtipos de tramas como son: Beacons, Probe Request, Probe Response, Association Request, Association Response, Reas. Request, Reas. Response, Authentication, DE authentication, Acknowledgement, Request to Send, Clear to Send y Data. Estos datos se detallan de cada uno de los dispositivos conectados a los access point con su respectiva dirección Mac.

### Figura 66

*Contador de tramas por dispositivos.*

	No	MAC_DISPO	PERCENT	N_PROBES_REQ	N_PROBES_RESP	N_ASS_REQ	N_ASS_RESP	N_REASS_REQ	N_REASS_RESP
1	1	01:00:5e:7f:ff:fa	0.239378	0	0	0	0	0	0
2	2	33:33:00:00:00:01	0.299222	0	0	0	0	0	0
3	3	7a:e9:84:d0:b3:...	1.01735	0	0	0	0	0	0
4	4	2c:2b:f9:48:62:57	47.3968	0	0	0	0	0	0
5	5	9c:ad:97:c9:bb:...	50.3291	0	0	0	0	0	0
6	6	01:80:c2:00:00:13	0.0598444	0	0	0	0	0	0
7	7	74:40:bb:0c:a1:4f	0.0598444	0	0	0	0	0	0
8	8	01:00:0c:cc:cc:cc	0.0598444	0	0	0	0	0	0
9	9	02:0f:b5:7c:65:8a	0.0598444	0	0	0	0	0	0
10	10	24:1b:7a:7c:65:8a	0.239378	0	3	0	0	0	0
11	11	33:33:ff:6e:42:da	0.239378	0	0	0	0	0	0

Por último, en la Figura 67 se muestra la tabla “Contador de tramas totales” la cual permite visualizar el detalle de las tramas de administración, control y datos. Esta

tabla muestra el número total de las tramas y su respectiva equivalencia en porcentaje para identificar que trama o tramas son las que más envía cada Access Point.

**Figura 67**

*Sección Contador de trama totales.*

características por ap		contador tramas por ap		contador tramas por dispositivo		contador tramas totales		
No	SSID	TOTAL	N_ADMIN	% ADMIN	N_CONTROL	% CONTROL	N_DATOS	% DATOS
1	CELERITY_BRAVO	1785	1114	62.409	587	32.8852	84	4.70588
2	Claro_FERNADOOSORIO	65	63	96.9231	0	0.0	2	3.07692
3	Claro_VALENCIA0015117285	30	29	96.6667	0	0.0	1	3.33333
4	Claro_RAMOS0007811299	12	12	100.0	0	0.0	0	0.0
5	Claro_NELSONIMBAQUING	5	4	80.0	0	0.0	1	20.0
6	Claro_VELASTEGUI0000105465	2	2	100.0	0	0.0	0	0.0
7	Omni_lite656540	19	5	26.3158	0	0.0	14	73.6842
8	SOFIA_CNT	1009	459	45.4906	21	2.08127	529	52.4281
9	NETLIFE-Carrillo_2GEXT	41	40	97.561	0	0.0	1	2.43902
10	NETLIFE-Carrillo	7	6	85.7143	0	0.0	1	14.2857

## Capítulo IV

### **Captura de Tráfico de Datos y Análisis de Resultados**

En este capítulo se desarrollarán escenarios de prueba del aplicativo desarrollado en Python en comparación con el software Wireshark, lo cual permitirá realizar un análisis comparativo y permitirá encontrar el margen de error del aplicativo desarrollado.

### **Pruebas de Compatibilidad con el Controlador de Acrylic**

En las pruebas realizadas entre el controlador Acrylic y Python en Windows con los diferentes tipos de adaptadores inalámbricos, se verifica que dependiendo de la compatibilidad de la tarjeta con el controlador acrylic (ver tabla de Tarjetas compatibles en modo monitor a travez del controlador de acrylic), el controlador permite visualizar diferente tipo de información que transmite cada AP.

Del mismo modo el acceso a la configuración del control panel ubicado en parte izquierda del programa desarrollado, se activará únicamente cuando la tarjeta seleccionada sea compatible con los drivers de acrylic, y en el caso de no activarse el control panel del programa la tarjeta automáticamente permitirá la captura de paquetes en saltos de frecuencia.

### **Adaptador Inalámbrico AirPcap NX**

El adaptador inalámbrico AirPcap NX debido a la buena compatibilidad que mantiene con Windows y con el controlador de acrylic permite visualizar la frecuencia, el canal y la potencia de cada Acces Point, así como también la encriptación, el cifrado y la autenticación.

Del mismo modo el acceso a la configuración del control panel ubicado en parte izquierda del programa desarrollado se activará únicamente cuando la tarjeta sea



seleccionada, y permitirá configurar el escenario en específico para la captura de los paquetes.

En la Figura 68 se puede observar los valores entregados y tabulados por el programa.

**Figura 68**

*Captura del trafico 802.11 mediante la tarjeta AirPcap NX.*

The screenshot shows the 'Sniffer' application window. On the left is a control panel with buttons for 'Abrir\_conexion', 'AirPcap USE wireless capture adapter nr. 00', and 'Borrar Base Datos'. Below these are settings for 'Control Panel', 'Modo\_seleccionado: Modo Canal Fijo', 'Canal Seleccionado: 1', and options for 'Selecion Canal Fijo' (2.4 GHz, 5 GHz) and 'Salto Frecuencia' (2.4 GHz, 5 GHz). On the right is a table with the following data:

caracteristicas por ap	contador tramas por ap	contador tramas por dispositivo	contador tramas totales				
SSID	MAC_AP	ENCRIPACION	CIFRADO	AUTENTICACION	POTENCIA(dBm)	CANAL	FRECUENCIA(MHz)
1 -NT	bcc0b0f658b18	TKIP CCMP	WPA2	PSK	-58	2412	1
2 -...	3c378674806c	TKIP CCMP	WPA2	PSK	-68	2437	6
3 -Cerrillo	94049c673280	TKIP CCMP	WPA2	PSK	-72	2437	6

### **Adaptador Inalámbrico TP-LINK TL-WN722N**

El adaptador inalámbrico TP-LINK TL-WN722N con chipset Atheros debido a la buena compatibilidad que mantiene con el controlador de acrylic permite visualizar la frecuencia, el canal y la potencia de cada Acces Point, así como también la encriptación, el cifrado y la autenticación.

Este adaptador captura automáticamente en satos de frecuencia, cabe recalcar que mediante el control panel del programa desarrollado no se puede modificar los parámetros de captura.

En la Figura 69 se puede observar los valores entregados y tabulados por el programa.

**Figura 69**

*Captura del trafico 802.11 mediante la tarjeta Tp-Link TL-Wn722n.*

características por ap		contador tramas por ap		contador tramas por dispositivo		contador tramas totales		
SSID	MAC_AP	ENCRIPCIÓN	CIFRADO	AUTENTICACIÓN	POTENCIA(dBm)	CANAL	FRECUENCIA	
1 SOFIA_CNT	bc:c0:f9:8b:18	TKIP CCMP	WPA2	PSK	-55	2412	1	

### Adaptador Inalámbrico LB-Link BI-wn150ah

El adaptador inalámbrico LB-Link BI-wn150ah con chipset RALINK debido a la limitada compatibilidad que mantiene con el controlador de acrylic permite visualizar, la encriptación, el cifrado y la autenticación, este adaptador inalámbrico, no muestra información sobre la frecuencia, el canal y la potencia de cada Access Point y automáticamente captura en satos de frecuencia, cabe recalcar que mediante el control panel del programa desarrollado no se puede modificar los parámetros de captura.

En la Figura 70 se puede observar los valores entregados y tabulados por el programa.

### Figura 70

*Captura del trafico 802.11 mediante la tarjeta Lb-Link BI-em150ah.*

No	SSID	MAC_AP	ENCRIPCIÓN	CIFRADO	AUTENTICACIÓN
1	NETLIFE-ALFRANCIS-EXT	06:6f:13:2c:d0:4f	WPA2	CCMP	PSK
2	NETLIFE-ALFRANCIS	cc:bb:fe:89:15:c0	WPA2	TKIP CCMP	PSK
3	HUAWEI-QD94_2_4GEXT	b0:95:75:2d:cba:f	WPA2	TKIP CCMP	PSK

### Obtención de Tráfico Wifi

Para la obtención de datos se utilizó el adaptador inalámbrico AirPcap NX y el software desarrollado en Python, así como también un generador de tráfico.

La recolección de los datos se la realizó en la Urbanización El Limonar 2 y 3 ubicado en la ciudad de Quito en donde existe un amplio número de Access Point

puesto que es un entorno residencial, lo cual permitirá obtener una mayor variedad de dispositivos, así como diferentes tipos de datos a capturar.

Las capturas fueron realizadas durante 7 días por un lapso de 60 minutos continuos en dos franjas horarias diferentes, la primera franja horaria de 08h00 a 09h00 y la segunda de 19h00 a 20h00, se realizó la captura en estos horarios debido a que la cantidad de usuarios, así como de datos capturados fue mayor que en otras horas del día.

Adicional a las capturas de datos en franjas horarias, se realizó una simulación de inyección de tráfico para determinar el margen de error del aplicativo desarrollado.

### **Análisis de Resultados**

Para determinar la eficacia del programa desarrollado en Python se analizará el error de los datos obtenidos mediante Wireshark con respecto a los datos obtenidos mediante el aplicativo desarrollado.

Entre los datos analizados se encuentran: tramas de control, tramas de administración, tramas de datos, tipo de encriptación y el canal de los puntos de acceso.

### **Análisis de Datos**

#### ***Protocolos de Seguridad***

Durante la captura del tráfico se encontraron 2 redes inalámbricas que trabajaban con encriptación WEP, 8 redes con WPA2-TKIP, 6 redes WPA2-CCPM-TKIP y 32 redes con WPA2-CCMP.

En la Figura 71 se puede identificar que más del 70% de las redes utilizan el tipo de seguridad WPA2 el cual cifra la información mediante el uso de AES lo que permite tener una mayor protección ante ataques en las redes inalámbricas domésticas.

**Figura 71**

*Protocolos de seguridad escaneados.*

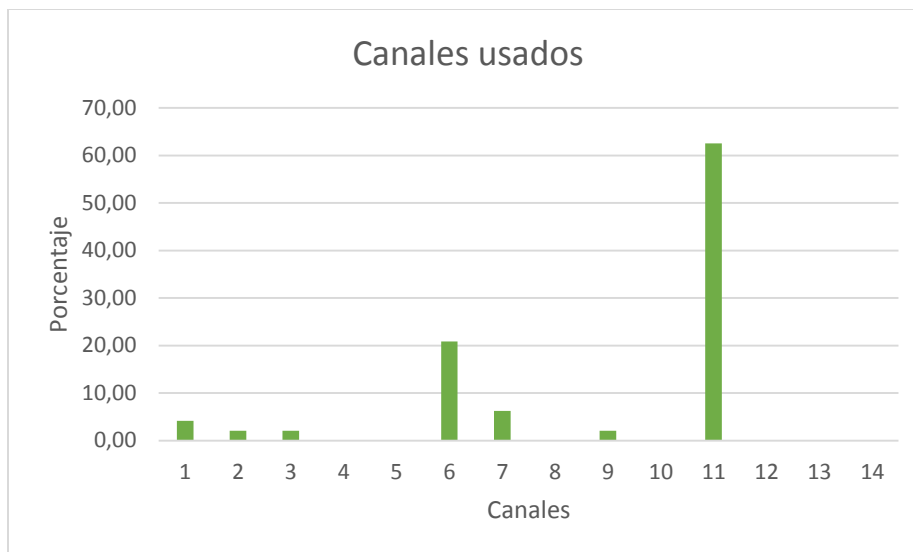
**Canales**

Durante las capturas del tráfico realizadas se encontró que los canales usados por los usuarios son el canal 6 con el veinte por ciento (20%) y el canal 11 con el 60 por ciento (60%) aproximadamente, eso se debe a que los canales 1, 6 y 11 no presentan interferencia co-canal, únicamente interferencia de canales adyacentes.

En la Figura 72 se puede identificar que el ochenta por ciento (80%) de los AP trabajan en el canal 6 y 11. Además que los canales 4, 5, 10, 12, 13 y 14 son canales que no se utilizan.

**Figura 72**

**Usuarios conectados a los diferentes canales.**



### **Eficiencia del Aplicativo**

Para determinar la eficiencia del aplicativo se calculó el error entre de las tramas de datos, control y administración obtenidas por el aplicativo con respecto a las tramas obtenidas mediante el software Wireshark, siendo las tramas obtenidas por Wireshark las tramas reales y las tramas obtenidas por el aplicativo desarrollado como un valor estimado.

### **Pruebas Mediante la Captura de Tráfico Real**

La captura de tráfico real se realizó mediante la tarjeta AirPcap NX durante dos horas del día en una urbanización de la ciudad de Quito, este tráfico capturado es generado por diferentes Access Point.

A continuación, se detalla el porcentaje de error por cada trama del tráfico real capturado.

### ***Tramas de Administración***

- **Beacons;** se detalla el porcentaje de error de las tramas beacon obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 3 de errores.

**Tabla 3**

*Porcentaje de error las tramas Beacons.*

Día	1	2	3	4	5	6	7	Promedio
<b>Mañana</b>	0,55	2,48	1,5	1,7	1,82	1,34	3,91	1,90
<b>Tarde</b>	2,07	2,02	2,71	3,91	1,11	2,74	3,69	2,61

- **Probe Request:** se detalla el porcentaje de error de las tramas Probe Request obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 4 de errores.

**Tabla 4**

*Porcentaje de error las tramas Probe Request.*

Día	1	2	3	4	5	6	7	Promedio
<b>Mañana</b>	4,96	3,07	3,47	1,41	1,58	3,48	3,85	3,12
<b>Tarde</b>	0,26	1,41	3,76	2,38	1,19	2,33	1,87	1,89

- **Probe Response:** se detalla el porcentaje de error de las tramas Probe Response obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 5 de errores.

**Tabla 5**

*Porcentaje de error las tramas Probe Response.*

Día	1	2	3	4	5	6	7	Promedio
<b>Mañana</b>	1,52	1,22	1,11	1,17	2,66	3,89	3,86	2,20

<b>Tarde</b>	4,15	2,55	3,49	2,91	2,12	1,68	3,01	2,84
--------------	------	------	------	------	------	------	------	------

- **Authentication:** se detalla el porcentaje de error de las tramas Authentication obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 6 de errores.

**Tabla 6**

*Porcentaje de error las tramas Authentication.*

<b>Día</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>Promedio</b>
<b>Mañana</b>	0	0	0	0	3,15	0	0	0,45
<b>Tarde</b>	0	1,56	0	0	0	0	0	0,22

- **DE authentication:** se detalla el porcentaje de error de las tramas DE authentication obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 7 de errores.

**Tabla 7**

*Porcentaje de error las tramas DE authentication.*

<b>Día</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>Promedio</b>
<b>Mañana</b>	0	0	0	0	0	0	0	0
<b>Tarde</b>	0	0	0	0	0	0	0	0

- **Association Request:** se detalla el porcentaje de error de las tramas Association Request obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 8 de errores.





<b>Tarde</b>	0	0	0	0	0	0	0	0
--------------	---	---	---	---	---	---	---	---

- **Reassociation Response:** se detalla el porcentaje de error de las tramas Reassociation Response obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 11 de errores.

**Tabla 11**

*Porcentaje de error las tramas Reassociation Response.*

<b>Día</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>Promedio</b>
<b>Mañana</b>	0	0	0	0	0	0	0	0
<b>Tarde</b>	0	0	0	0	0	0	0	0

**Tramas de Control**

- **Acknowledgement:** se detalla el porcentaje de error de las tramas Acknowledgement obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 12 de errores.

**Tabla 12**

*Porcentaje de error las tramas Acknowledgement.*

<b>Día</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>Promedio</b>
<b>Mañana</b>	0,77	2,19	3,7	2,72	1,32	3,31	1,86	2,27
<b>Tarde</b>	4,49	3,24	3,66	3,69	2,79	3,86	1,61	3,33

- **Request to Send:** se detalla el porcentaje de error de las tramas Request to Send obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 13 de errores.

**Tabla 13**

*Porcentaje de error las tramas Request to Send.*

Día	1	2	3	4	5	6	7	Promedio
<b>Mañana</b>	2,44	3,84	3,67	2,02	3,54	3,62	2,85	3,14
<b>Tarde</b>	0,27	2,59	2,3	3,12	2,51	1,03	3,92	2,25

- **Clear to Send:** se detalla el porcentaje de error de las tramas Clear to Send obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 14 de errores.

**Tabla 14**

*Porcentaje de error las tramas Clear to Send.*

Día	1	2	3	4	5	6	7	Promedio
<b>Mañana</b>	4,91	1,1	3,47	2,84	1,21	2,68	1,82	2,58
<b>Tarde</b>	0,63	1,19	0	2,83	0	1,43	1,98	1,15

### **Tramas de Datos**

- **Data:** se detalla el porcentaje de error de las tramas Data obtenidas en el transcurso de la mañana y tarde. A continuación, se muestra la Tabla 15 de errores.

**Tabla 15**

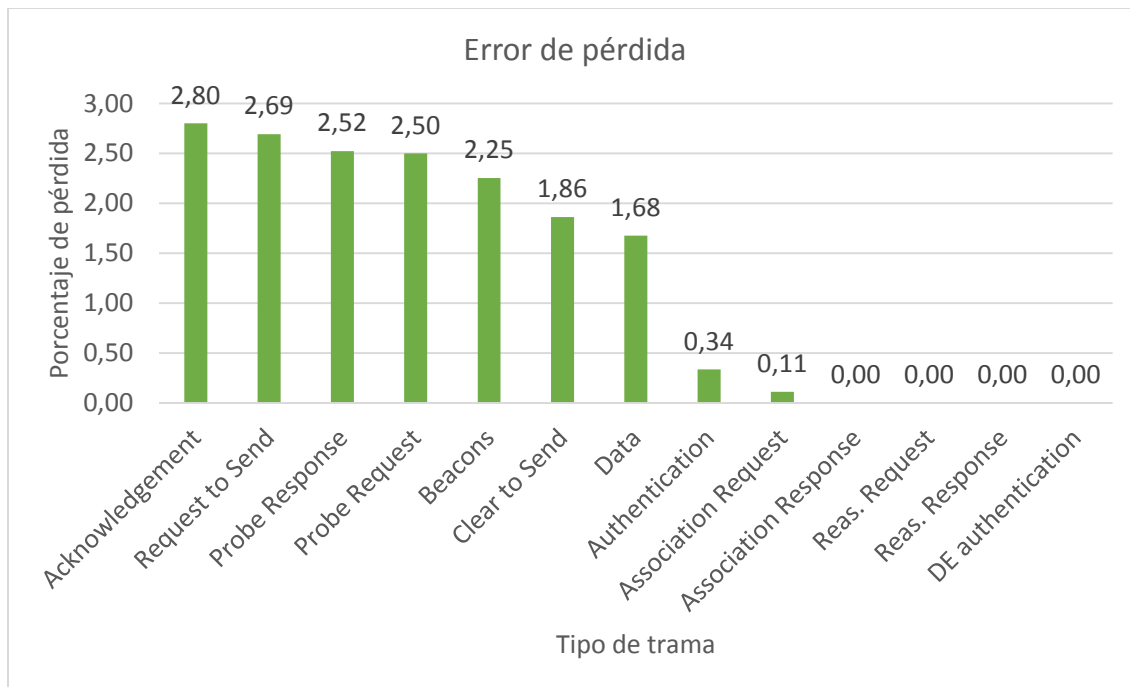
*Porcentaje de error las tramas Data.*

Día	1	2	3	4	5	6	7	Promedio
<b>Mañana</b>	0,12	1,7	1,13	2,81	0,11	1,89	2,05	1,40
<b>Tarde</b>	1,94	3,42	2,19	1,05	1,75	1,73	1,56	1,95

En la Figura 73 se muestran las pérdidas de todas las tramas y se pueda establecer que la trama con mayor pérdida son los Acknowledgement con un 2.80% de error debido a que en ciertas mediciones el valor de captura era menor a 10 paquetes y el valor capturado difería en 1 o 2 paquetes al valor real mostrado por Wireshark lo que implica que el error se incremente.

**Figura 73**

*Porcentaje total de pérdidas en las tramas capturadas.*



## Pruebas Mediante la Inyección de Tráfico

La inyección de tramas se realizó mediante una máquina virtual en LINUX, para ello se realizó una captura de paquetes generados mediante tráfico real para replicar los archivos a inyectar por cada tipo de trama.

El escenario de pruebas para la inyección de tráfico se la realizo con 200, 500 y 1000 paquetes por tres ocasiones no consecutivas, la inyección de tráfico se la realizó a una distancia de 1 metro de entre las tarjetas de inyección y captura.

A continuación, se muestran los siguientes tipos de tramas inyectados mediante SSID: Network\_Esteban y BSSID: 8A:BB:24:1A:74:C1 con la tarjeta modelo TP-LINK TL-WN722N.

### Tramas de Administración

- **Beacons:** se detalla el porcentaje de error de las tramas Beacons con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas.

A continuación, se muestra la Tabla 16 de errores.

**Tabla 16**

*Porcentaje de error las tramas Beacons.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	1,73	0	0,57
Inyección 3	0	0	0	0

- **Probe Request:** se detalla el porcentaje de error de las tramas Probe Request con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 17 de errores.

**Tabla 17**

*Porcentaje de error las tramas Probe Request.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0,87	0,29
Inyección 3	0	0	0	0

- **Probe Response:** se detalla el porcentaje de error de las tramas Probe Response con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 18 de errores.

**Tabla 18**

*Porcentaje de error las tramas Probe Response*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	1,56	0,53	0.69

- **Authentication:** se detalla el porcentaje de error de las tramas Authentication con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 19 de errores.

**Tabla 19**

*Porcentaje de error las tramas Authentication.*

Paquetes	200	500	1000	Promedio
Inyección 1	4,28	0	0	1,42
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

- **DE authentication:** se detalla el porcentaje de error de las tramas DE authentication con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 20 de errores.

**Tabla 20**

*Porcentaje de error las tramas DE authentication.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

- **Association Request:** se detalla el porcentaje de error de las tramas Association Request con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 21 de errores.

**Tabla 21**

*Porcentaje de error las tramas Association Request.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

- **Association Response:** se detalla el porcentaje de error de las tramas Association Response con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 22 de errores.

**Tabla 22**

*Porcentaje de error las tramas Association Response.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

- **Reassociation Request:** se detalla el porcentaje de error de las tramas Reassociation Request con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 23 de errores.

**Tabla 23**

*Porcentaje de error las tramas Reassociation Request.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

- **Reassociation Response:** se detalla el porcentaje de error de las tramas Reassociation Response con inyección de tráfico mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 24 de errores.

**Tabla 24**

*Porcentaje de error las tramas Reassociation Response.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

### ***Tramas de Control***

- **Acknowledgement:** se detalla el porcentaje de error de las tramas Acknowledgement con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 25 de errores.



**Tabla 25**

*Porcentaje de error las tramas Acknowledgement.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

- **Request to Send:** se detalla el porcentaje de error de las tramas Request to Send con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 26 de errores.

**Tabla 26**

*Porcentaje de error las tramas Request to Send.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

- **Clear to Send:** se detalla el porcentaje de error de las tramas Clear to Send con inyección de tráfico obtenido mediante las tres inyecciones no consecutivas. A continuación, se muestra la Tabla 27 de errores.

**Tabla 27**

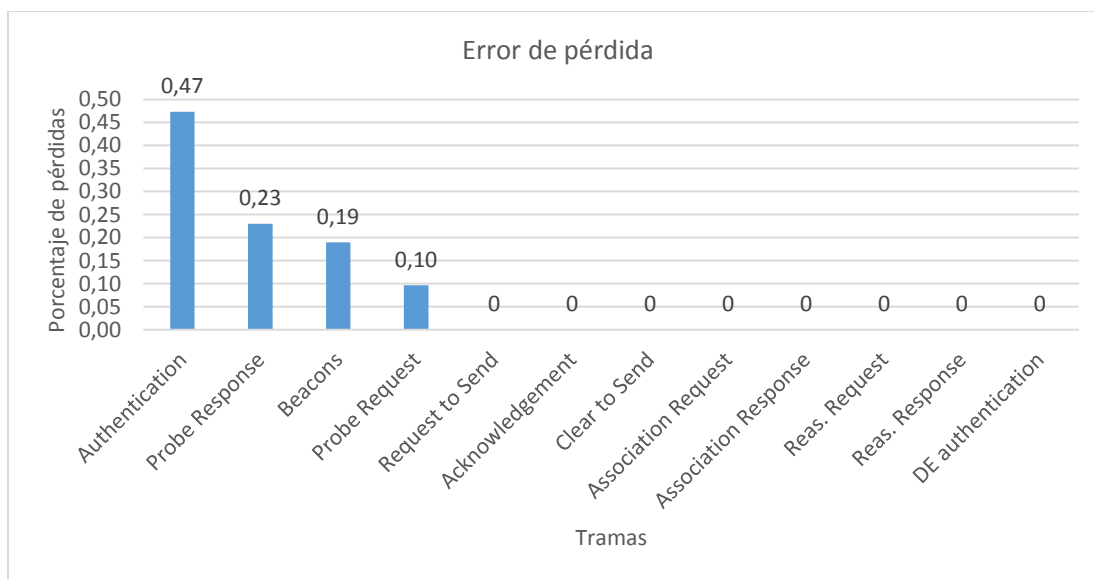
*Porcentaje de error las tramas Clear to Send.*

Paquetes	200	500	1000	Promedio
Inyección 1	0	0	0	0
Inyección 2	0	0	0	0
Inyección 3	0	0	0	0

En la Figura 74 se muestran las pérdidas de todas las tramas y se puede establecer que la trama con mayor pérdida es la de Authentication con promedio de 0,47% de pérdidas.

**Figura 74**

*Porcentaje total de pérdidas en las tramas capturadas con la inyección.*



Finalmente, en una prueba rápida de captura de tráfico en la pestaña de “contador por dispositivo” se puede observar en la Figura 75 que existen las direcciones MAC de los dispositivos de los usuarios conectados al AP y sus respectivos paquetes clasificados por su subtipo.

**Figura 75**

*Direcciones Mac de los dispositivos vinculados a sus respectivos Ap.*

características por ap		contador tramas por ap		porcentaje tramas por ssid	características por dispositivos		contador tramas por dispositivo		contador tramas total
No	SSID	MAC_DISPO	PERCENT	N_PROBES_REQ	N_PROBES_RESP	N_ASS_REQ	N_ASS_RESP	N_REASS_REQ	
1	NETLIFE-DANNY	33:33:00:00:00:0c	62.5	0	0	0	0	0	
2	NETLIFE-DANNY	01:00:5e:7f:ff:fa	12.5	0	0	0	0	0	
3	NETLIFE-MAE	ff:ff:ff:ff:ff:ff	25.0	0	0	0	0	0	

## Capítulo V

### Conclusiones y Recomendaciones

#### Conclusiones

- Se desarrolló una aplicación que permite caracterizar tramas 802.11 en redes inalámbricas compatible con el sistema operativo de Windows, la cual tuvo un correcto funcionamiento en cada uno de los escenarios que fue probado.
- Se pudo notar que el comportamiento de las tarjetas varía dependiendo del fabricante. El modelo Ralink inicialmente captura una mayor cantidad de paquetes, mientras que el modelo Atheros captura pasado un intervalo de tiempo, pero acumula una mayor cantidad de paquetes, esto se debe a que el fabricante del controlador indica que la compatibilidad con adaptadores Atheros es buena mientras que para modelos Ralink es limitada. El adaptador de red Airpcap que usa el driver "Airpcap 4.1.3", captura la mayor cantidad de tramas de forma constante, además posee librerías que permiten seleccionar el canal en el que se desea capturar paquetes tanto en la banda de 2.4 GHz y 5GHz, canales de 20 o 40 MHz, entre otras opciones.
- Se utilizó el paquete pandas para la clasificación de tramas por cada SSID hallado. El método read\_sql fue de gran utilidad ya que permite hacer consultas en la base de datos y almacenar esta información en Dataframes que son estructuras que facilitan la ubicación de datos importantes como direcciones MAC de origen, destino, subtipos de tramas y contadores.
- Para el salto de frecuencia en la banda de 2.4 GHz se creó una lista de canales con un salto de 5 para evitar solapamientos entre ellos. Para la selección de ancho de banda de 40 MHz la librería airpcap.h proporciona una función que selecciona un canal principal y secundario de 20 MHz con un salto de 4 canales

de manera automática para evitar solapamientos por lo que fue necesario determinar los canales que se encuentren en el extremo de la banda de 2.4 o 5 GHz para condicionar que el canal secundario sea menor al primario en estos casos.

- Para llamar a las funciones de la librería "airpcap.h" desde Python se utilizó el módulo ctypes que contiene métodos para cargar archivos .dll y crear tipos de datos equivalentes en el lenguaje c, de esta forma se pudo abrir conexiones con la tarjeta airpcap y utilizar funciones que permitieron cambiar de canal, seleccionar anchos de banda e incluso prender un led para comprobar la comunicación. Se comprobó que la versión 2.7 de Python permitió crear una conexión con el adaptador de red mientras que la 3.8 no, por esta razón se tuvo que crear un ejecutable que se inició desde la versión más actual de Python.
- Al incluir más condiciones de búsqueda en las sentencias SQL de actualización el porcentaje de error se redujo en el caso de tráfico inyectado ya que las direcciones MAC de origen y destino coincidían en varios registros de la tabla de administración, control y datos por lo que fue necesario especificar la búsqueda por los nombres de los subtipos.
- El análisis de resultados presento que al realizar una captura de tráfico real en promedio el aplicativo desarrollado mantuvo un error del uno coma veinte y nueve por ciento (1,29%) a diferencia del error con tráfico generado, el cual fue de cero coma cero ocho por ciento (0,08%), denotando que el error máximo en el tráfico real fue de dos coma ochenta por ciento(2,80%) perteneciente a las tramas de Acknowledgement, seguido de las tramas Request to Send con dos coma sesenta y nueve por ciento (2,69%), Probe Response con dos coma cincuenta y dos por ciento (2.52%), Probe Request con dos coma cincuenta cinco por ciento (2.50%), Beacons con dos coma veinte y cinco por ciento(2,25%), Clear to

Send con uno coma ochenta y seis por ciento (1,86%), Data con uno coma sesenta y ocho por ciento (1,68%), Authentication con cero coma treinta y cuatro por ciento(0,34%), Association Request con cero coma once por ciento (0,11%), Association Response con cero por ciento(0%), Reas. Request con cero por ciento (0%), Reas. Response con cero por ciento (0%) y DE authentication con cero por ciento (0%) y con la inyección de tráfico las tramas que presentaron error fueron las de Authentication con cero coma cuarenta y siete por ciento (0,47%), Probe Response con cero coma veinte y tres por ciento (0,23%), Beacons con cero coma por ciento (0,19%) y Probe Request con cero coma diez por ciento (0,10%).

- Los errores generados en las capturas de las tramas no son mayores al 5% y este error se debe a la ejecución de los hilos de captura y procesamiento ya que estos hilos tardan milisegundos en ejecutarse y poder enviar los datos a la base de datos para su posterior visualización en el programa desarrollado.

### **Recomendaciones**

- Antes de iniciar la inyección de paquetes es recomendable usar el programa aireplay-ng con la opción -9 para comprobar que el adaptador de red soporte este modo.
- Se debe actualizar a la versión más reciente de Scapy ya que se solucionan problemas de compatibilidad o añadir nuevas funciones para extraer información de paquetes capturados.
- La propiedad que tienen los objetos de la clase Scapy para extraer el tipo de cifrado o encriptación usualmente detecta información errónea por lo que es recomendable interpretar la información de las Capas Dot11EltRSN o Dot11MicrosoftWPA.

- Se puede usar el comando `help` para obtener más información acerca de los argumentos que requieren las funciones utilizadas de `scapy`.
- Los nombres que representan la información acerca de la trama 802.11 son sensibles a mayúsculas y minúsculas por lo que se recomienda utilizar el comando `ls()` ya que este lista el nombre exacto de las capas.
- Es recomendable trabajar en un entorno virtual en Python para contar con versiones de paquetes y módulos específicos para el proyecto. Además, esto facilita crear un archivo con los nombres de las dependencias cuando se necesite compartir el proyecto.
- Se puede leer los comentarios dentro de la librería “`airpcap.h`” ya que aquí se especifica qué tipo de datos se recibe como parámetro, valores de retorno y el propósito de cada función.
- Para comprobar la comunicación se puede encender varios diodos led del adaptador de red `Airpcap`, o imprimir en pantalla el valor retornado al abrir una conexión ya que un valor igual a cero representa falso y 1 verdadero en el lenguaje C.

### **Trabajos Futuros**

- Distribuir el sistema para que un computador capture y haga un pre procesamiento de paquetes mientras que un segundo computador realice la búsqueda y clasificación de la información en bases de datos para incrementar la velocidad de procesamiento de la información.
- Explorar el paquete `scapy` de forma que se pueda modificar el comportamiento de la función `sniff` para integrarla con la clase `Qthread` de `pyqt5` de modo que se pueda compartir información entre clases de este paquete.

- Crear un driver NDIS para Windows que permita un comportamiento más estable de las tarjetas de red en modo monitor.



## Bibliografía

- Andreu, F., Pellejero, I., & Lesta, A. (2006). *Fundamentos y Aplicaciones de Seguridad en Redes WLAN: Fundamentos y Aplicaciones de Seguridad*. España: Marcombo.
- Carballar, J. A., & Carballar Falcón, J. A. (2010). *WI-FI. Lo que se necesita conocer*. España: RC Libros.
- Enriquez, A., Hamilton, J., & Taha Ahmed, B. (2014). *Banda Ancha Inalámbrica: WiMAX*. España: OmniaScience.
- Geier, E. (5 de Noviembre de 2015). *jmvinazza.wordpress.com*. Obtenido de <https://jmvinazza.wordpress.com/2015/11/05/cmo-configurar-los-canales-wifi-para-un-mejor-rendimiento-de-la-red/>
- Gonzalez, V. (2014). *Diseño e implementación de un sistema de monitoreo basado en SNMP para la red nacional de tecnología avanzada*. BOGOTÁ D.C.
- Holla, V. (2017). *WPA Information Element | Hitch Hiker's Guide to Learning. Hitch Hiker's Guide to Learning*.
- Hostinger. (2019). *Como funciona Mysql*. Obtenido de <https://www.hostinger.es/tutoriales/wp-content/uploads/sites/7/2019/04/como-funciona-mysql.jpg>
- Imgur. (2015). *Wireshark*. Obtenido de <https://i.imgur.com/272Aehv.png>
- Imgur. (2015). *Microsoft Message Analyzer*. Obtenido de <https://i.imgur.com/04r7Rd1.png>
- Imgur. (2015). *tcpdump*. Obtenido de <https://i.imgur.com/QOpceNO.png>

- Intercompras. (2015). *intercompras-a.akamaihd.net*. Obtenido de <https://n9.cl/8cpzg>
- Íñigo, J., & Barceló, J. (2009). *Estructura de redes de computadores*. Barcelona: Editorial UOC.
- Itesa. (2017). *www.itesa.edu.mx*. Obtenido de <https://n9.cl/z8si>
- Jiménez, T. (2015). *UF1875 - Gestión de recursos, servicios y de la red de comunicaciones*. España: Editorial Elearning, S.L.
- Junco, G. (2012). *www.monografias.com*. Obtenido de <https://n9.cl/pkpl>
- Lara, E. (2020). *Desarrollo de un aplicativo para caracterizar tramas 802.11 en redes inalámbricas utilizando software*. Latacunga.
- Loayza, C. (2010). *Estudio del Rendimiento del Estándar 802.11 en la Comparación con Dispositivos con el Estándar 802,11B/G en la Transmisión de Datos*. Riobamba.
- Manzano, V., & Vásquez, D. (2014). *Red Inalámbrica tipo malla (WNM) estándar 802.11 de transmisión y la optimización de cobertura en los Colegios de la Provincia de Tungurahua*. Ambato.
- Menéndez, S. (2016). *UF1880 - Gestión de redes telemáticas*. España: Editorial Elearning, S.L.
- Morales, E., & Córdova, E. (2010). *Las Redes Inalámbricas y su Incidencia en la Interconexión de las Redes Industriales en los Laboratorios de la Carrera de Ingeniería Industrial en Procesos de Automatización de la Facultad de Ingeniería en Sistemas Electrónica e Industrial*. Ambato.
- Mouteira, R. (2004). *Instalacion De Redes Informaticas e Ordenadores*. España: Ideaspropias Editorial S.L.

- Oliva, N. (2013). *Redes de comunicaciones industriales*. España: Editorial UNED.
- Páez, T. (2015). *Implementación de un prototipo de sistema de análisis de tráfico de redes 802.11 utilizando la minicomputadora Raspberry PI*.
- PC Tecnología. (2017). *pc-tecnologia*. Obtenido de <https://n9.cl/712kd>
- Postigo, A. (2020). *Seguridad informática (Edición 2020)*. España: Ediciones Paraninfo, S.A.
- Riverbed. (2009). *Riverbed AirPcap*. Singapur: Riverbed.
- Rojas, B. (2019). *Python para principiantes: Aprenda Python en 5 días con orientación paso a paso y ejercicios prácticos*. Babelcube Inc.
- Security, T. (13 de 12 de 2020). *Tarlogic*. Obtenido de <https://www.tarlogic.com/programas-wifi/acrylic-wifi/#:~:text=Driver%20NDIS%3A%20Acrylic%20instala%20un,con%20Wireshark%20y%20Cain%20%26%20Abel>.
- Silva, M. (2017). *Receptar mensajes de correo electrónico, entre otras*. Mexico.
- Sincables. (2018). *LB-Link BI-wn150ah*. Obtenido de <https://sincables.com.ec/wp-content/uploads/2018/11/BL-WN150AH-2.jpg>
- Stanfanick, G. (2018). *A closer look at WiFi Security IE (Information Elements)*.
- TpLink. (2015). *static.tp-link*. Obtenido de <https://n9.cl/eed9o>
- TP-Link. (13 de 12 de 2020). *TP-Link*. Obtenido de TP-Link: <https://www.tp-link.com/mx/home-networking/adapter/tl-wn722n/>

Wikimedia. (2020). *wikimedia.org*. Obtenido de  
([https://upload.wikimedia.org/wikipedia/commons/thumb/9/93/Trama\\_802.11.png/600px-Trama\\_802.11.png](https://upload.wikimedia.org/wikipedia/commons/thumb/9/93/Trama_802.11.png/600px-Trama_802.11.png)).

Wisborg, J., & Okuno, M. (2019). *Pro MySQL NDB Cluster*. Apress.

Wordpress. (2011). *seguridadyredes*. Obtenido de  
<https://seguridadyredes.files.wordpress.com/2011/05/tshark-1.png?w=621&zoom=2>

**Anexos**