Realizar un análisis de las vulnerabilidades y mecanismos de explotación asociados a redes wifi abiertas.

Cristian Steven Pedraza Castro

Carlos Steeven Herrera González

Universitaria Agustiniana

Facultad de Ingenierías

Programa de Ingeniería en Telecomunicaciones

Bogotá D.C

2018

Realizar un análisis de las vulnerabilidades y mecanismos de explotación asociados a redes wifi abiertas.

Cristian Steven Pedraza Castro

Carlos Steeven Herrera González

Director

Francisco Clemente Valle Díaz

Trabajo de grado para optar al título Ingeniería en Telecomunicaciones

Universitaria Agustiniana

Facultad de Ingenierías

Programa de Ingeniería en Telecomunicaciones

Bogotá D.C

2018

Resumen

El presente trabajo de investigación tiene como tema principal el análisis de las vulnerabilidades de las redes wifi abiertas y el tráfico de información que se genera durante una conexión entre el punto de acceso inalámbrico y un usuario. Se realizaron diferentes laboratorios dentro de la Universitaria Agustiniana, donde mediante el uso diferentes equipos y componentes de telecomunicaciones se generaron diferentes resultados que ayudan a concluir el comportamiento, manejo y funcionamiento de los usuarios al momento de realizar una conexión hacia una red wifi abierta.

El desarrollo de la investigación tuvo como pilar de desarrollo el análisis de los diferentes protocolos que actúan en una conexión wifi tales como UDP, TCP-IP y protocolos de seguridad como SSL, WPA, WPA2, WPE donde por medio de simulación de redes wifi abiertas en ambientes controlados y realizando ataques de HOMBRE EN MEDIO poniendo a prueba los aplicativos más utilizados por los estudiantes dentro de la Universitaria Agustiniana tales como WhatsApp, Facebook, correos electrónicos, aplicativos de uso institucional como el Siga Uniagustiniana, las aulas virtuales y el aplicativo web de la biblioteca.

Después de realizadas todas las pruebas y con el trafico capturado, el cual fue analizado con la herramienta WIRESHARK dentro del sistema operativo KALI LINUX, se puede observar cuales de estos aplicativos utilizados por directivos, docentes, personal administrativo y estudiantes son los más vulnerables.

Palabras Clave: Wireshark, Red wifi abierta, Ataque hombre en medio, Kali Linux y Hacking.

Abstract

The main topic of this research work is the vulnerability analysis of open Wi-Fi networks and the information traffic that is generated during a connection between the wireless access point and a user. Different laboratories were carried out within the Augustiniana University, where by using different telecommunications equipment and components different results were generated that help to conclude the behavior, management and operation of the users when making a connection to an open Wi-Fi network.

The development of the research had as a pillar of development the analysis of the different protocols that act in a Wi-Fi connection such as UDP, TCP-IP and security protocols such as SSL, WPA, WPA2, WPE where by simulation of open Wi-Fi networks in controlled environments and making attacks of HOMBRE EN MEDIO by testing the applications most used by students within the University of Augustin such as WhatsApp, Facebook, emails, applications and institutional application such as the SIGA Uniagustiniana, virtual classrooms and the web application from the library.

After carrying out all the tests and with the traffic captured, which was analyzed with the WIRESHARK tool within the KALI LINUX operating system, it can be seen which of these applications used by managers, teachers, administrative staff and students are the most vulnerable.

Keywords: Wireshark, Open wifi network, Man attack in between, Kali Linux and Hacking.

Tabla de contenido

1. Introducción

Actualmente en nuestro país millones de personas quieren estar comunicadas virtualmente desde cualquier lugar, esto lo hacen aún más estando en sus estaciones de trabajo, universidades, colegios, instituciones y lugares públicos, etc. Con la continua implementación de redes WIFI abiertas promovidas por los actuales planes de gobierno en ámbitos de conectividad, se plantea este proyecto conociendo las necesidades con las que cuenta cada persona y buscando informar a cada usuario el riesgo que conlleva conectarse a una red wifi abierta.

Para ello se decidió realizar un análisis minucioso de las aplicaciones con más frecuencia de uso. Se analizaron redes sociales como WhatsApp, Facebook, correos electrónicos y aplicativos de uso institucional como el Siga Uniagustiniana, las aulas virtuales y el aplicativo web de la biblioteca, donde mediante un diseño de red Wifi-Abierta implementada por los autores del proyecto de grado y utilizando un sistema operativo KALI LINUX con el analizador de tráfico WireShark, se creó un esquema de simulación con dos dispositivos uno siendo el atacante y el otro siendo la victima dentro de una red. El ataque implementado es conocido como HOMBRE EN MEDIO.

Se pone en análisis las herramientas que normalmente se usan para conocer cuáles de ellas cuentan con un protocolo de seguridad que garantice la confiabilidad de datos personales del usuario y poder generar recomendaciones de seguridad en cuanto el uso de este tipo de conexiones abiertas.

2. Problema de investigación

2.1 Planteamiento del problema

Con el mundo conectando cada vez más dispositivos a las redes wifi que se encuentran en el entorno, se generan grandes cantidades de tráfico por minuto. Se estima que un grupo importante de personas se exponen regularmente a los peligros de enviar información a través de una red sin cifrado, esta situación se presenta en parte debido a la falta de conocimiento respecto de las vulnerabilidades asociadas a las redes wifi-abiertas, razón por la cual se observa la necesidad de trabajar en temas asociados a la concientización de la ciudadanía en general. Con el presente trabajo se pretende avanzar en dicho campo al exponer los mecanismos de explotación que pueden ser utilizados para obtener información de los usuarios de las redes wifi-abiertas.

2.2 Pregunta de investigación

Siendo las redes inalámbricas (wifi) abiertas un recurso usado altamente por el público, ¿Se encuentra en riesgo la seguridad (confidencialidad) de los datos de los usuarios?

3. Justificación

En los últimos años las redes inalámbricas abiertas se han convertido en una tendencia tecnología usualmente utilizada para proveer conectividad al público en diferentes lugares como entidades, establecimientos, institutos, centros de recreación públicos, entre otros, se genera una gran cantidad de tráfico de información que queda expuesta a las vulnerabilidades propias de las redes abiertas. Por este motivo se busca analizar a detalle qué tipo de información es vulnerable y como se pueden tomar acciones para mejorar la seguridad al utilizar redes abiertas.

.

4. Objetivos

4.1 Objetivo general

Analizar a detalle el tráfico de información y seguridad de una red wifi abierta.

4.2 Objetivos específicos

- Realizar un estudio de la información captable en una red wifi abierta.
- Encontrar los puntos débiles que afectan la información en una red wifi abierta
- Explotar las vulnerabilidades encontradas al utilizar redes wifi-abiertas.
- Plantear recomendaciones que mejoren la seguridad de los usuarios al utilizar redes abiertas.

5. Marco de referencia

5.1 Marco teórico

En la actualidad, se encuentran dos escenarios donde se acumula el mayor uso de las redes inalámbricas (WLAN). Aplicación que se enfoca en el ámbito residencial y empresarial, ya que se encontró que en estos dos entornos se facilita el uso pues tiene mayor movilidad y facilita la conectividad sin tener la necesidad de un cableado, lo más importante que ofrece esta tecnología es llegar a las diferentes zonas donde es muy complicado utilizar medios físicos. La seguridad es uno de los aspectos a considerar al implementar este tipo de redes, una de las diferencias entre una red cableada y una (WLAN), es que la red cableada solo necesita un medio físico para conectarse, y la red WLAN el único medio de propagación es el aire. Lo que más preocupa a en cuestión de seguridad, es que puede haber terceros utilizando o teniendo también un acceso a cada uno de nuestros datos. (González A, Beltrán D, y Fuentes E, 2016)

Lo que se concluye en este artículo es que existen diferentes mecanismos de seguridad que son aplicables, como es el sistema de terminales de usuario basándose en la dirección MAC de este, no siendo el más eficiente y buscando otras opciones encontraron la actualización y el equipamiento de WPA o siendo la mejor opción el mecanismo WPA2 puesto que es menos vulnerable y presenta un sistema de autenticación con mayor eficiencia en comparación. (González A, Beltrán D, y Fuentes E, 2016)

En el siguiente artículo, elaborado por Kotz D, Essien K, nos da a conocer algunos de los patrones que hacen uso de las redes inalámbricas (WLAN). El propósito de la investigación es el documentar y mostrar algunos de los resultados del rastro completo y las actividades que se realizaron en una LAN inalámbrica de producción. (Kotz D, Essien K, 2002)

Dentro de las muestras que se realizaron día a día, hora a hora y semana a semana, se dieron cuenta de diferentes situaciones durante la captura de datos. La primera fue a la hora de visualizar algunas subredes cruzadas las cuales fueron uno de los mayores problemas, después de que se realizaron más estudios concluyeron que el mayor uso de las redes WLAN empresariales es durante la noche. Otras de las conclusiones generadas, fue que donde hay mayor concentración de personas conectadas a una

red inalámbrica es en lugares de residencia y donde hay un menor índice de personas conectadas es en edificios con una red cableada muy bien estructurada. (Kotz D, Essien K, 2002)

Una de las importancias de este trabajo es que hoy en día las comunicaciones inalámbricas son parte importante de la vida de cada una de las personas, lo cual nos hace pensar que, en un corto lapso de tiempo, la sociedad sea más fuerte en las comunicaciones digitales. La pregunta más importante que se realizó durante la investigación realizada por Avella J, Bohórquez J, Peña N, y Bermúdez G, es que las personas hacen uso de comunicaciones inalámbricas, pero ninguna de ellas se ha puesto en la tarea de ver cuál es la importancia de ellas. El principal objetivo fue utilizar un robot móvil, que en cada uno de los lugares donde él se encontrara, pudiera realizar una comunicación con cada una de estas redes y capturara datos (trafico) para después poder ser analizado. (Avella J, Bohórquez J, Peña N, y Bermúdez G, 2009).

Los resultados que exponen en el artículo fue de mayor satisfacción ya que cumplieron con alguno de sus propósitos, por otra parte, dejaron un trabajo a futuro, en el que exponen otro sistema de antenas para hacer la captura de los datos. (Avella J, Bohórquez J, Peña N, y Bermúdez G, 2009)

Otra investigación de análisis del tráfico dentro de una red WI-FI dirigida por Carroll J, Hernández C, y Puerta G quienes publican los diferentes resultados que se presentan en los algoritmos ARFIMA y SFARIMA donde se determinará cual es el mejor predictor del tráfico en una red. Los primeros experimentos que utilizaron fueron con un dispositivo encargado de capturar datos en cada uno de los nodos del Municipio de Chía Cundinamarca, lo cual encontraron que cada uno de estos nodos tienen una velocidad de 2 Mbps. Con una cobertura de 105 Kilómetros cuadrados aproximadamente, para el primer experimento de captura de datos tomaron 24 muestras en dos horas con intervalos de 5 minutos. (Carroll J, Hernández C, y Puerta G, 2012)

Lo que se concluyó en este trabajo fue que el modelo SFARIMA presenta una gran ventaja frente al modelo ARFIMA, pero una de las características que no gusto mucho es que este modelo conlleva a un mayor consumo de recursos. Pero para el caso de visualizar el tráfico en una red WI-FI el modelo ideal es el SFARIMA ya que toda la cantidad de puntos en la captura coincide con el tráfico estimado en las practicas anteriores. (Carroll J, Hernández C, y Puerta G, 2012)

La investigación arroja resultados de un análisis de seguridad de redes WLAN en la ciudad de Tunja Boyacá Colombia enfocada en toda la ciudad, distribuida en diferentes puntos, usando técnicas de captura de información con enfoque hacia redes masivas, se genera un diagnóstico de seguridad informática. Se encontró una representación significativa de redes inalámbricas de empresas públicas, privadas, entidades educativas y hogares ubicados geográficamente en diferentes sectores de la ciudad. (Monsalve J, Aponte F, Chaparro F, 2015)

Como se esperaba, se identificó diferentes niveles de riesgo informático provenientes en las configuraciones de algunos dispositivos de diferentes entidades públicas, privadas o residenciales, y se generaron algunas recomendaciones respecto a los datos captados. (Monsalve J, Aponte F, Chaparro F, 2015)

Continuando más a detalle con los puntos débiles de las redes, el artículo "WEP, WPA and WPA2 encryption protocols vulnerability on wireless networks with Linux platform" se muestra una comparativa de características de los tres principales estándares de seguridad en una red inalámbrica IEEE 802.11: WEP, WPA y WPA2. Con un análisis detallado del algoritmo RC4 se indican las vulnerabilidades de los sistemas de cifrado y comparando de manera analíticamente las ventajas que nos presentan los métodos de acceso de las redes wifi. Se logra concluir y determinar por qué se han tenido que crear las actualizaciones de los protocolos y que ha variado en la implementación de estos métodos. (Moreno W, Mosquera D, Rivas E, 2015)

5.2 Marco conceptual

5.2.1. Redes inalámbricas.

Se considera una comunicación inalámbrica, la red que sin el uso de cables permite generar una conexión entre los usuario o dispositivos. Una red inalámbrica es la cual permite conectar diversos dispositivos utilizando el aire como medio de transmisión generando un proceso más rápido y con flexibilidad. Estas pueden clasificarse dependiendo el criterio que se quiera evaluar. (e-reding, s.f.)

Las redes inalámbricas también se pueden clasificar en los siguientes tipos que muestra la siguiente figura.

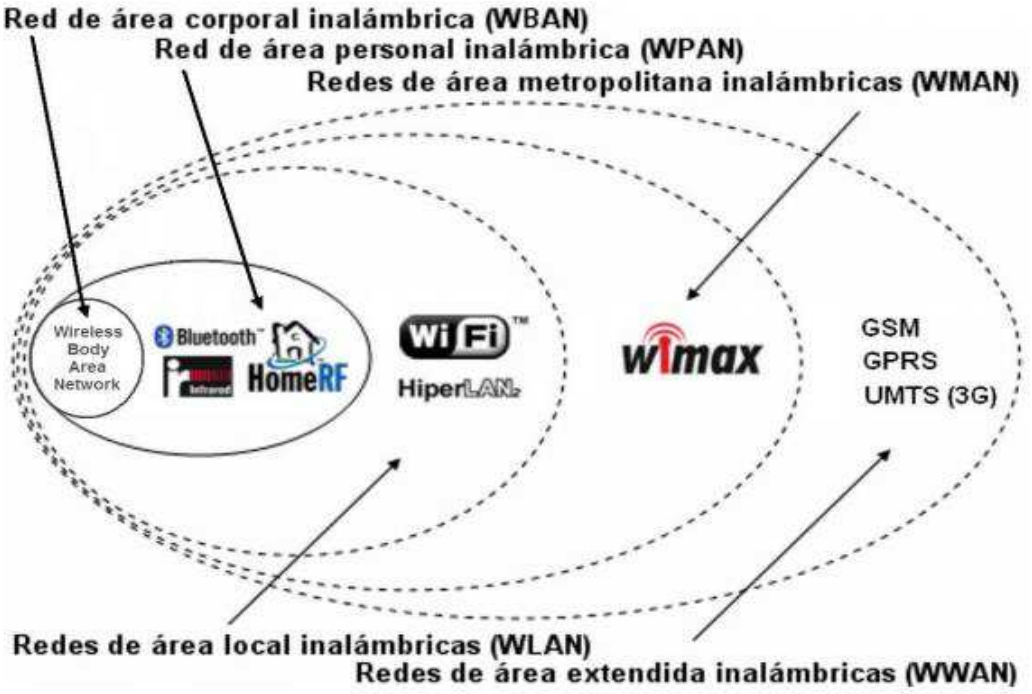

Figura 1 Diagrama de redes inalámbricas (Katheryne; & Romero, 2012)

5.2.2 Administración de redes.

Se define como administración de redes, al conjunto de técnicas que permiten generar una organización, control, toma de precauciones para mantener un funcionamiento pleno de la red.

Los objetivos de administrar una red y de tener una persona designada y encargada de esta tarea, es poder definir estrategias de mejora y planificación en temas de infraestructura y eficacia, con funciones primordiales como: Detección y aislamiento de fallas, evaluación del tráfico en la red, mantenimientos de configuraciones y está en la capacidad y habilidad del administrador en demostrar su proactividad para darle una mejor administración a la red. Esta labor de administración tiene como objetivos el generar herramientas manuales o automáticas para monitorear o y controlar la red en su totalidad, añadiendo estrategias de contención y optimización de la infraestructura de la red en gestión. (Banda T, Alexander B, 2006)

5.2.3 Protocolos de seguridad de red.

Los protocolos de seguridad en redes son algoritmos y procesos que se aplican en todo tipo de redes las cuales añaden un agregado de seguridad para proteger la información que circula por la red. Estas se pueden aplicar en redes inalámbricas (wlan) en protocolos como los que muestra la figura 2. (González A, Beltrán D, Fuentes E, 2016)

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

Figura 2 Generalidades de protocolos de seguridad *(Ciens, s.f.)*

Existen principalmente dos aspectos a tener muy en cuenta en la seguridad de redes: la autenticación y el cifrado. (González A, Beltrán D, Fuentes E, 2016)

Por otro lado, se considera como autenticación el proceso de verificar la identidad del usuario involucrado en la petición de conexión. Se usa para evitar que una entidad maliciosa asuma identidades falsas comprometiendo así la privacidad y seguridad de la información. (González A, Beltrán D, Fuentes E, 2016)

5.2.4 Cifrado en redes.

Proceso por el cual la información transmitida por un sistema de comunicación es tratada y codificada de diferentes maneras, con el fin de no arriesgar la seguirá y que la información sea interceptada por actores ajenos a la línea de comunicación. Estos métodos de cifrado en redes inalámbrica (Wlan), son altamente usados en la mayoría de las redes y se dividen principalmente en (acens, 2012):

5.2.4.1.Cifrado WEP. Tiene como objetivo, proporcionar confidencialidad, autentificación y control de acceso (acens, 2012)

5.2.4.2.Cifrado WPA. Fue el protocolo de seguridad lanzado para mejorar los problemas del protocolo WEP (acens, 2012)

5.2.4.3.Cifrado WPA+ Psk. Es el protocolo de la familia WAP más sencillo recomendado para hogares y pequeñas empresas (acens, 2012)

5.2.4.4.Cifrado WPA empresarial. Usado por empresas con mayor infraestructura tecnológica por la complejidad del proceso de autenticación haciendo uso de certificados o usuarios alojados en servidores. (acens, 2012)

5.2.4.5.Cifrado WPA2. Es el actual y más seguro protocolo de encriptación presentando bastantes mejoras ante su predecesor el protocolo WPA (acens, 2012)

En la figura 3, se puede observar el uso de los protocolos mas usados en el año 2013 en la ciudad de mexico.

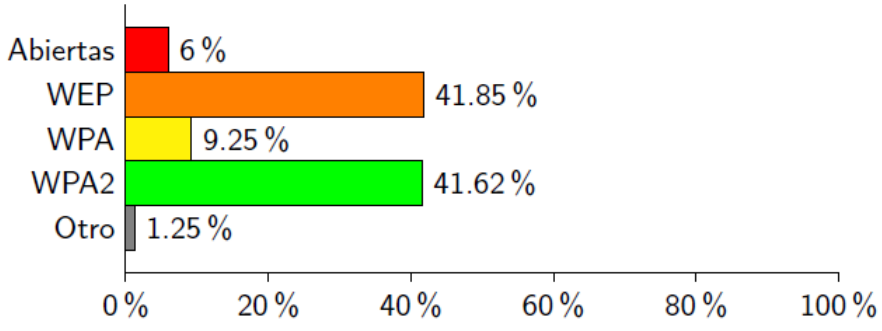

Figura 3 Uso de los protocolos de encriptación (Websec, 2013)

5.2.5 Auditoria en redes inalámbricas.

Es el proceso mediante el cual se analiza a detalle el tráfico e infraestructura, con el objetivo de proporcionar una visión detallada de la red WIFI, buscar puntos débiles de la red wifi que permitan obtener información de manera clandestina analizando la seguridad y protocolos de cifrado.

5.3 Marco legal

Tabla 1

Leyes aplicadas al problema de investigación.

Normatividad	Articulo	Descripción
Ley 72 de 1989 del Ministerio de la información y la comunicación de Colombia.	1	El Gobierno Nacional, por medio del Ministerio de Comunicaciones, adoptará la política general del sector de comunicaciones y ejercerá las funciones de planeación, regulación y control de todos los servicios de dicho sector, que comprende, entre otros: - los servicios de telecomunicaciones. - los servicios informáticos y de telemática. - los servicios especializados de telecomunicaciones o servicios de valor agregado. - los servicios postales. (MinTic, Ministerio de telecomunicaciones , 1989)
	2	Se entiende por telecomunicaciones, toda transmisión, emisión o recepción de signos, señales, escritos y sonidos, datos o información de cualquier naturaleza, por hilo, radio, medios visuales u otros sistemas electromagnéticos. (MinTic, Ministerio de telecomunicaciones , 1989)
	4	Los canales radioeléctricos y demás medios de transmisión que Colombia utiliza o pueda utilizar en el ramo de las telecomunicaciones son propiedad exclusiva del Estado. (MinTic, Ministerio de telecomunicaciones , 1989)
	11	El Ministerio de Comunicaciones establecerá políticas de normalización, y de adquisición de equipos y soportes lógicos de telecomunicaciones acordes con los avances tecnológicos, para garantizar la interconexión de las redes y el inter-funcionamiento de los servicios de telecomunicaciones. (MinTic, Ministerio de telecomunicaciones , 1989)

Ley 1900 de 1990 del Ministerio de la información y la comunicación de Colombia.	14	La red de telecomunicaciones del Estado es el conjunto de elementos que permite conexiones entre dos o más puntos definidos para establecer la telecomunicación entre ellos, y a través de la cual se prestan los servicios al público. Hacen parte de la red los equipos de conmutación, transmisión y control, cables y otros elementos físicos, el uso de los soportes lógicos, y la parte del espectro electromagnético asignada para la prestación de los servicios y demás actividades de telecomunicaciones. (MinTic, Ministerio de telecomunicaciones , 1990)
	18	El espectro electromagnético es de propiedad exclusiva del Estado y como tal constituye un bien de dominio público, inajenable e imprescriptible, cuya gestión, administración y control corresponden al Ministerio de Comunicaciones de conformidad con las leyes vigentes y el presente Decreto. (MinTic, Ministerio de telecomunicaciones , 1990)
	19	señala que las facultades de gestión, administración y control del espectro electromagnético comprenden, entre otras, las actividades de planeación y coordinación, la fijación del cuadro de frecuencias, la asignación y verificación de frecuencias, el otorgamiento de permisos para su utilización, la protección y defensa del espectro radioeléctrico, la comprobación técnica de emisiones radioeléctricas, el establecimiento de condiciones técnicas de equipos terminales y redes que utilicen en cualquier forma el espectro radioeléctrico, la detección de irregularidades y perturbaciones, y la adopción de medidas tendientes a establecer el correcto y racional uso del espectro radioeléctrico, y a restablecerlo en caso de perturbación o irregularidades. (MinTic, Ministerio de telecomunicaciones , 1990)
Ley 29 de 1990 del Ministerio de la información y la comunicación de Colombia.	2	La acción del Estado en esta materia se dirigirá a crear condiciones favorables para la generación de conocimiento científico y tecnología nacionales; a estimular la capacidad innovadora del sector productivo; a orientar la importación selectiva de tecnología aplicable a la producción nacional; a fortalecer los servicios de apoyo a la investigación científica y al desarrollo tecnológico; a organizar un sistema nacional de información científica y tecnológica; a consolidar el sistema institucional respectivo y, en general, a dar incentivos a la creatividad, aprovechando sus producciones en el mejoramiento de la vida y la cultura del pueblo. (MinTic, Ministerio de telecomunicaciones , 1990)
		Las Tecnologías de la Información y las Comunicaciones (en adelante TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios,

Ley 1341 de 2009 del Ministerio de la información y la comunicación de Colombia.	6	que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, vídeo e imágenes. El Ministerio de Tecnologías de la Información y las Comunicaciones junto con la CRC, deberán expedir el glosario de definiciones acordes con los postulados de la UIT y otros organismos internacionales con los cuales sea Colombia firmante de protocolos referidos a estas materias. (MinTic, Ministerio de telecomunicaciones , 2009)
	32	Para manejar los recursos de la Agencia Nacional del Espectro, se podrán celebrar contratos de fiducia, con observancia de los requisitos legales que rigen esta contratación. En este caso, la fiduciaria manejará los recursos provenientes del presupuesto nacional y los demás que ingresen a la Agencia. El Director General de la Agencia coordinará el desarrollo y la ejecución del contrato de fiducia, a través del cual desarrollará las actuaciones que le sean propias. (MinTic, Ministerio de telecomunicaciones , 2009)
Concepto Jurídico del Ministerio de la información y la comunicación de Colombia.	622337	Reforma Tributaria en aspectos del Sector TIC. Los dispositivos móviles inteligentes excluidos del impuesto sobre las ventas son todos aquéllos que tienen como características: teclado completo táctil o físico, operan sobre sistemas operativos estándares actualizables, permiten la navegación en Internet, tienen conectividad WIFI, con acceso a tiendas de aplicaciones y soportan las aplicaciones hechas por terceros. (MinTic, MinTic, 2013)
Ley 1273 de 2009 del Ministerio de la información y la comunicación de Colombia		Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado “De la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (MinTic, MinTic, 2009)
Ley 1581 de 2012 del Ministerio de la información y la comunicación de Colombia		desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (MinTic, Ministerio de telecomunicaciones, 2012)

5.4 Marco metodológico

5.4.2 Tipo de investigación

La investigación cuantitativa se puede definir como el grupo de procedimientos y decisiones que tienen como finalidad señalar una conclusión exacta a través de magnitudes numéricas que puedan ser tratadas estadísticamente. Es necesario que para que sea usada este tipo de metodología investigativa, exista algún modelo matemático que represente una relación, debe ser lo más objetiva posible sin permitir que factores personales externos del investigador influyan en las decisiones o conclusiones de la investigación. (R Hernández, Fernández C, Baptista M, México 2010)

Por otra parte, se le conoce al método científico como el proceso a seguir para dar con un resultado esperado sin que los factores personales del investigador, dando como resultado una conclusión a un problema lo más objetiva posible. Se basa en 6 pasos los cuales se resumen en: Identificación de un problema, desechar los aspectos no esenciales al problema, recolección de datos relevantes al problema, generación de la hipótesis, comprobación de la hipótesis a través de pruebas y/o experimentos, conclusión general o respuesta al problema. (Gutiérrez S, 2006)

Por el tipo de rama investigativa perteneciente a los procesos que se desarrollarán, sabemos que los datos serán exactos y que no existe punto de interpretación intermedio o guiado por factores personales. Todo será medible por variables exactas y se realizará a través de procesos previamente estudiados y con hipótesis pactadas para cada prueba

A continuación, se presenta en la taba 2 el cuadro de experimentos investigativos a realizar.

Tabla 2

Cuadro de experimentos investigativos.

Objetivos Especificos	Instrumento	Población	Resultados
Implementar una red wifi de prueba, sobre la cual se capturará el trafico	Diseño de una red Wifi-abierta	Uniagustiniana	Se obtuvo una red wifi la cual se implementó para realizar las pruebas, la cual no tiene ningún sistema de cifrado de datos simulando una red wifi abierta
	AP E410 Cambium y describirlo y sus propiedades	Red wifi abierta llamada VIRUS-NO-CONECTARSE. La cual fue implementada con el AP (Access Point) E410 Cambium	Se realizaron captura de tráfico de datos en aplicaciones y sitios web más utilizados por una persona natural, por periodos de tiempo de 3 minutos.
	Verificar que tan vulnerables son los datos de una persona cuando se conecta a una red abierta	Se realizó un ataque llamado HOMBRE EN MEDIO en una red Wifi-abierta	El ataque se realizó con el fin de verificar que datos son vulnerables y verificar la seguridad de dichas aplicaciones

Identificar los elementos a utilizar con los cuales se va a capturar y analizar el trafico	Se utilizaron dos computadores uno siendo el atacante y el otro el atacado, un sistema operativo Kali Linux, una suit Aircrack y wiresharck, smartphones	Red Wifi abierta llamada VIRUS-NO-CONECTAR. y aplicaciones como el siga de la Universitaria, Facebook, Gmail, WhatsApp, aulas virtuales, revistas electrónicas.	Se evidencia que con estas herramientas se puede capturar y analizar el tráfico que circula sobre la red wifi seleccionada, las cuales se evidencio que unas de estas aplicaciones están cifradas y otras no, estas capturas se evidenciaran en la tabla de resultados. Se evidencia
Identidentificar alguna manera de mejorar la seguridad al navegar en redes wifi-abiertas	VPN a implementar	Uniagustiniana	se evidencia que el tráfico que se encuentra libre en algunas de estas aplicaciones ya tiene más seguridad, la cual se evidenciara en el cuadro de resultados

5.4.3 Etapas de proceso cuantitativo

Tabla 3

Características del enfoque Cuantitativo por fase.

Concepto	Definición
Idea	Muestra necesidades de medición y predicción.
Planteamiento del problema	Delimitado Concreto Cuestiones específicas Fija hipótesis.
Marco teórico	Corroboran hipótesis Congruente Aporta evidencia
Desarrollo de investigación	Secuencial Deductivo Objetivo
Recolección de datos	Análisis de datos Fundamenta en mediciones Variables
Análisis de datos	Graficas
Elaboración de reporte de resultados	Explicativo

6. Cronograma

Cronograma	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Actividades																				
Planteamiento de proyecto de investigación																				
Estado del arte																				
documentación y características técnicas a tener en cuenta según lo identificado en el estudio																				
Documentación de equipos definidos																				
Documentación del diseño																				
Documentación del diseño de la aplicación sobre el software utilizado																				
Documentos de equipos definidos																				
Documentación del Diseño																				
Documentación de pruebas a realizar (variables, métodos, medidores, etc.)																				
Documentación de resultados																				
Análisis de resultados																				
Conclusiones																				
Documentación																				
Presentación																				

Figura 4 Cronograma de actividades

7. Presupuesto

Tabla 4

Descripción presupuesto de recursos humanos

A. Recursos Humanos			
Perfil	Justificación	Cantidad	Valor
Estudiante	**Con este proyecto podremos detectar que tan vulnerable es una red WIFI abierta.**	**2**	2.000.000

Tabla 4

Descripción presupuesto hardware y software

B. Equipos		
Equipo	Justificación	Valor
• Antena con funcionalidades de modo promiscuo. • Computador portátil Intel core i5 2 generadion 4gb Ram	**Con este elemento se podrá lograr capturar los datos que viajan a través de una red WIFI abierta.** **Con este elemento se podrá realizar los ataques necesarios para la captura de información.**	$ 200.000 $ 500.000

C. Software		
Software	Justificación	Valor
• Linux Kali • Credenciales	**-Con este elemento podremos capturar analizar y encontrar que tan vulnerables son las redes Wifi-abiertas.**	$ 000000

Tabla 5

Descripción presupuesto de desplazamientos

Justificación	Cantidad	Costo Unidad	Valor
Ubicación objetiva donde se podrán realizar pruebas en controlados.	5	$ 20.000	$ 100.000

Tabla 6

Descripción presupuesto general

G. Presupuesto
Valor
$ 2.800.000

8. Resultados

Para el desarrollo de la investigación se recopilaron los siguientes datos relevantes para el cumplimiento de los objetivos planteados, logrando vulnerar 2 de las 3 aplicaciones nativas de la universitaria Uniagustiniana y evaluar la seguridad según los comunicados de 3 de las aplicaciones externas más usadas.

Tabla 7

Resultados pruebas realizadas

Matriz de análisis de resultados					
ID de la prueba	**Nombre de la prueba**	**Técnica de ataque realizada**	**Duración de la prueba (minutos de captura de información)**	**Tr afico Cifra do?**	**Observaciones**
HM-01	Hombre en medio Aulas Virtuales	Hombre en medio	0:03:00	NO	El trafico está totalmente interceptable y no está cifrado. Se logra capturar datos de acceso a la plataforma, información y material gráfico de la plataforma e información de usuarios relacionados en una misma aula virtual
HM-02	Hombre en medio Biblioteca Virtual	Hombre en medio	0:03:00	NO	El tráfico no está cifrado revelando en una red abierta la información más sensible para un usuario, su usuario y contraseña
HM-03	Hombre en medio Facebook App	Hombre en medio	0:03:00	SI	El tráfico se encuentra cifrado y cumple con los estándares básicos de seguridad, más sin embargo se encontró un tipo de desvío de tráfico hacia 2 direcciones ip sin ninguna asociación hacia Facebook.

HM-04	Hombre en medio Gmail app	Hombre en medio	0:03:00	SI	El trafico cumple con la seguridad necesaria básica de cifrado para evitar ataques de hombre en el medio.
HM-05	Hombre en medio Siga	Hombre en medio	0:03:00	SI/ NO	El tráfico se encuentra cifrado respondiendo de manera local desde la universidad, más sin embargo no se obliga al usuario a que la navegación sea de manera segura.
HM-06	Hombre en medio WhatsApp	Hombre en medio	0:03:00	NO	El trafico enviado desde la aplicación de WhatsApp efectivamente cumple con el cifrado punto a punto evitando que la información se pueda filtrar en redes abiertas sin ningún tipo de cifrado.

8.1. Prueba hombre en medio aulas virtuales Uniagustiniana

Dado el continuo desarrollo tecnológico el cual ha permitido modernizar y cambiar el punto de vista de la educación, han surgido plataformas que permiten tener clases en línea o apoyo a las asignaturas presenciales. Por este motivo y al ser una herramienta con bastante uso dentro de la universitaria Agustiniana, se realiza una verificación de que tan segura es respecto a la información

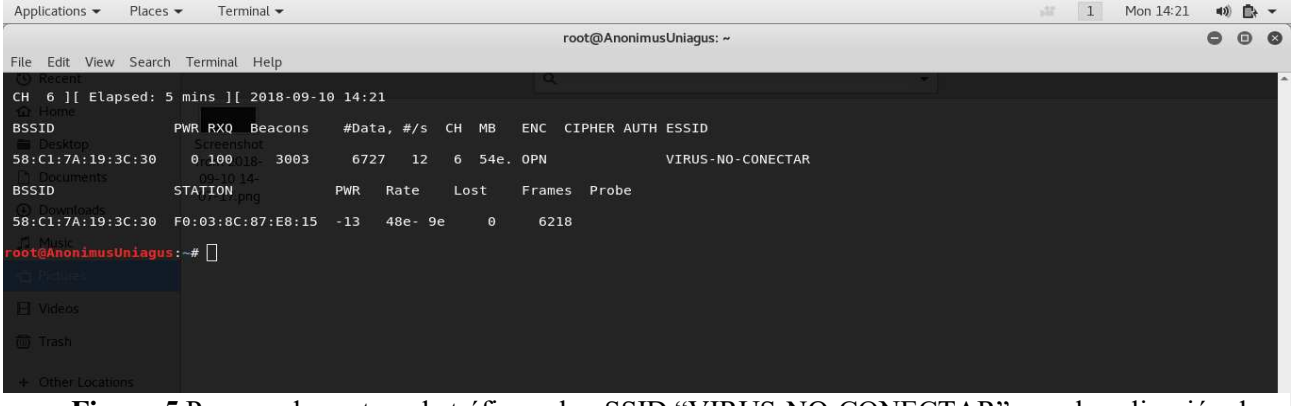

Figura 5 Proceso de captura de tráfico sobre SSID "VIRUS-NO-CONECTAR" para la aplicación de aulas virtuales.

de sus usuarios. realizó un ataque de hombre en el medio durante un rango de tiempo de 3 minutos enfocado el tráfico del aplicativo web de las aulas virtuales.

El trafico analizado, se encontró que el servicio de las aulas virtuales está alojado localmente en la red de la Universitaria Agustiniana.

Tabla 8

Numero de paquetes enviados al portal de aulas virtuales.

IP	Servicio	Numero de Paquetes	Porcentaje representativo en los datos capturados
172.16.0.151	Aulas Virtuales	2649	4,8%

De un total de 54950 paquetes capturados, 2649 son provenientes de la plataforma virtual de asignaturas y de los cuales el 100% es tráfico que no está cifrado. De este tráfico que no se encuentra cifrado se logró obtener información como lo es “Usuario” y “Password” de los usuarios, contenido

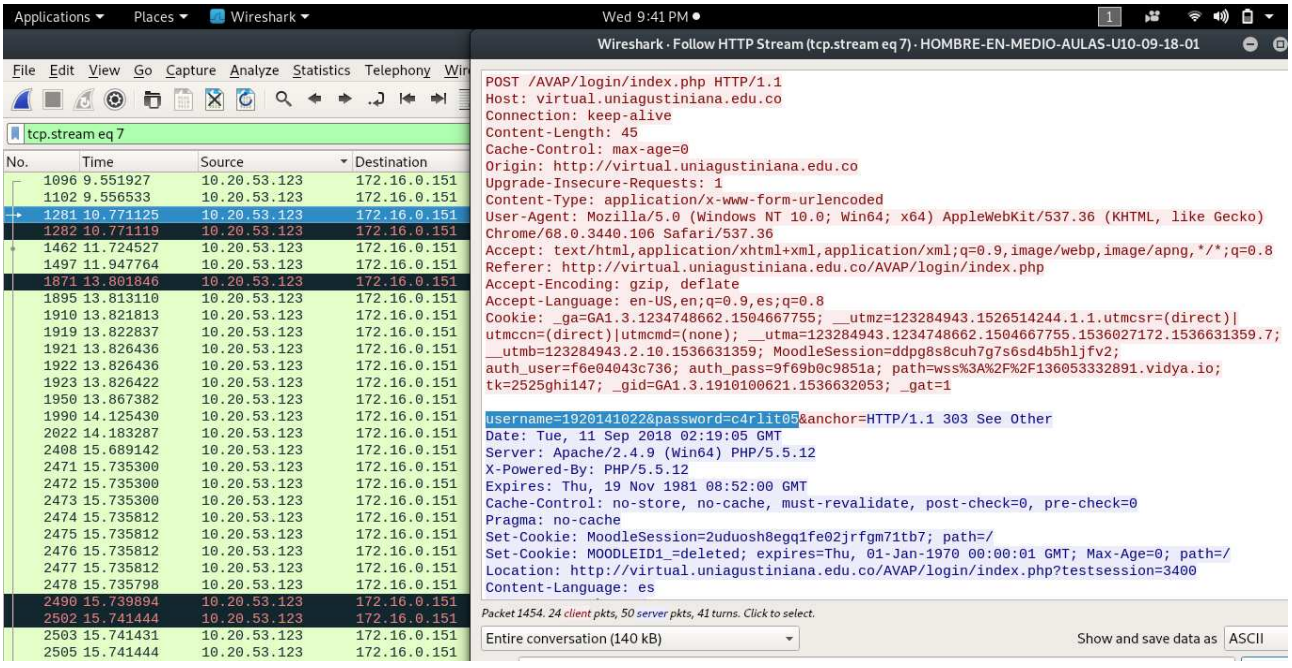

Figura 6 Trafico capturado para la prueba aulas virtuales agustinianas

grafico de los cursos o del material asignado a cada estudiante y datos de otros estudiantes asignados a una misma asignatura.

Se logró obtener el usuario y contraseña de uno de los investigadores (Usuario: 1920141021; Password: c4rlit05), y toda la información del curso preparatorio para el examen saber pro.

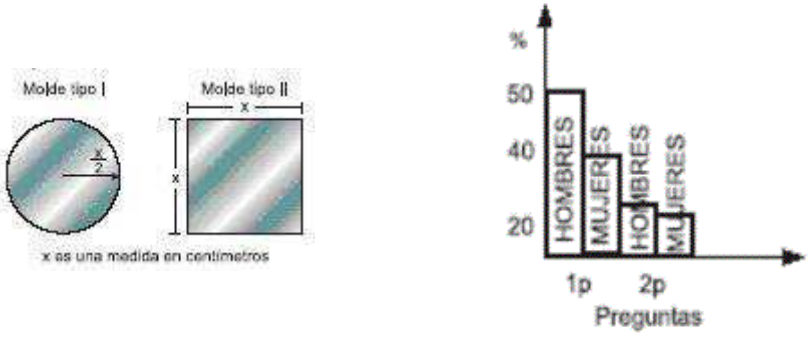

Figura 7 Gráficos capturados de las preguntas del simulacro del examen del saber pro 2018

También se logró capturar la foto de perfil de los usuarios vinculados a este examen preparatorio.

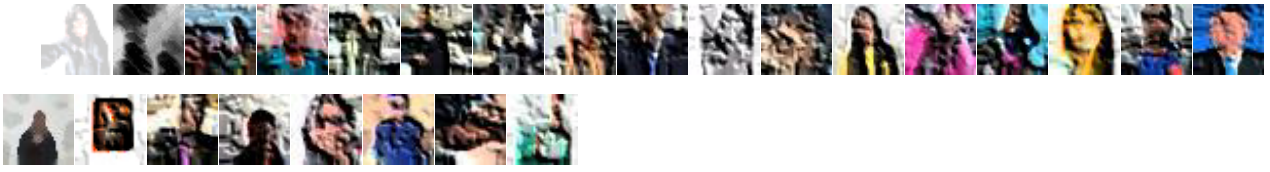

Figura 8 Captura de las fotos de identificación en la plataforma de los estudiantes asociados al simulacro del saber pro 2018

Toda esta información puede ser usada con muchos fines, y dado a la tendencia de los usuarios en usar la misma contraseña para diferentes servicios, se podría llegar a vulnerar demasiada información.

8.2. Prueba hombre en medio biblioteca virtual Uniagustiniana

Siendo los repositorios virtuales de la universidad un elemento en continuo uso gracias a promoción de los docentes en las diferentes áreas de conocimiento de la universitaria Agustiniana, se realiza una verificación de que tan seguro es el uso de este aplicativo dentro de una red Wifi abierta.

Se realizó un ataque de hombre en el medio durante un rango de tiempo de 3 minutos enfocado en la navegación a través del portal de la biblioteca virtual Agustiniana.

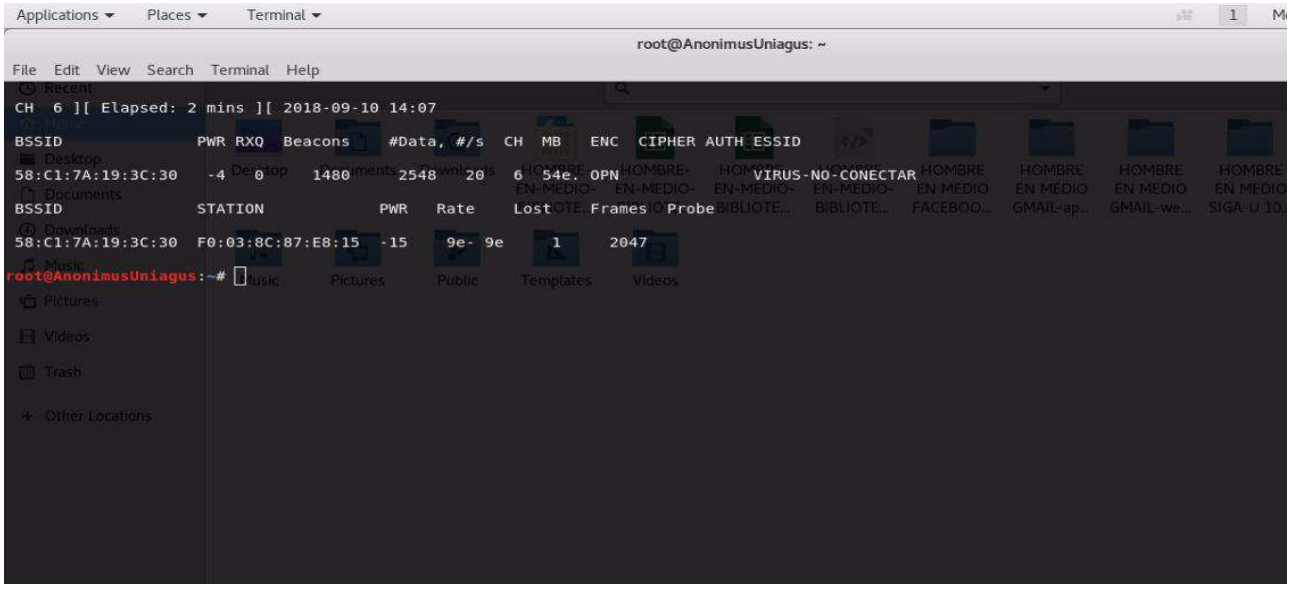

Figura 9 Proceso de captura de tráfico sobre SSID “VIRUS-NO-CONECTAR” para la aplicación de la biblioteca virtual.

Realizando el análisis a profundidad de la información capturada, se confirma que la mayor parte de este se encuentra sin cifrar, y entrando en más detalla revisando minuciosamente la dirección IP privada <172.16.0.98> que responde una gran cantidad de peticiones se encuentra la información más sensible para una persona, su usuario y contraseña.

Como se puede observar en la siguiente captura de pantalla, se detalla como el tráfico http revela completamente en que porta está navegando <http//:catalogobibliografico.uniagustiniana.edu.co>, su UserIS:1920141022 y su Password:1014278670.

La información revelada es parte de uno de los investigadores.

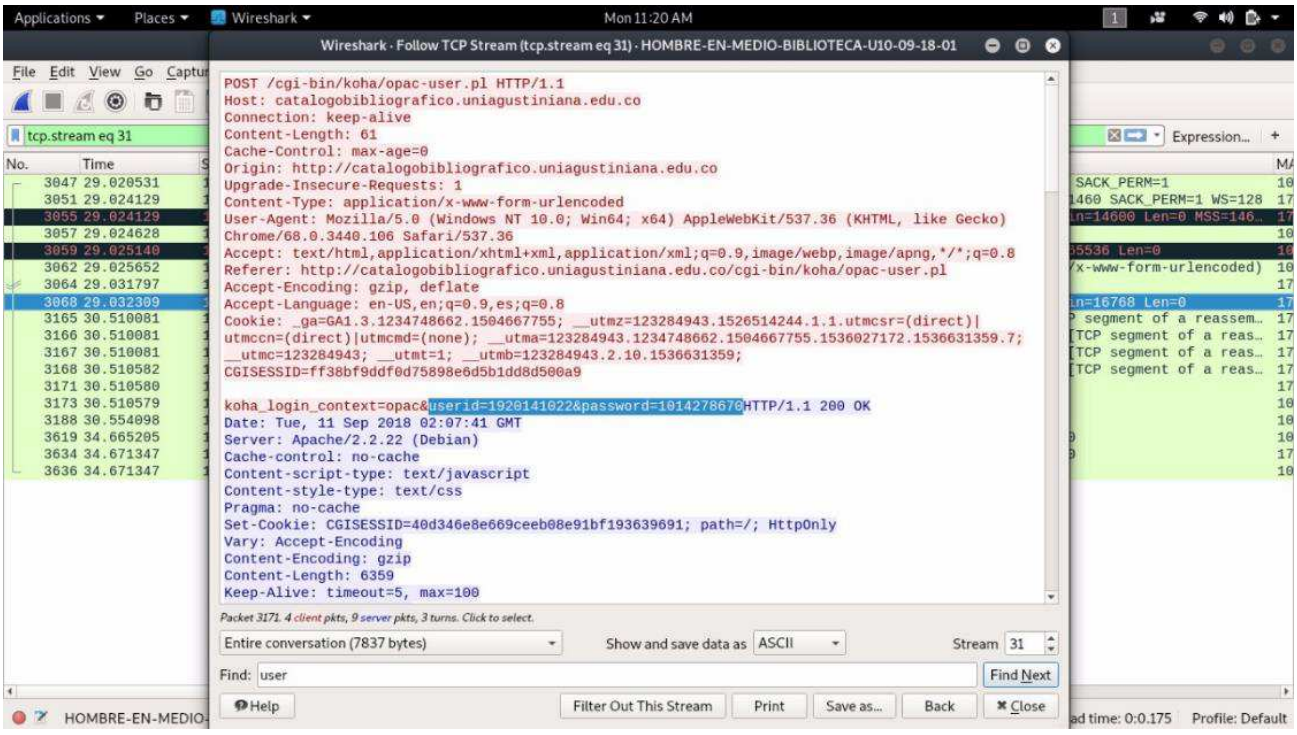

Figura 10 Información capturada del proceso de ingreso a la plataforma.

Analizando el tráfico restante se encuentra que en el proceso intervienen otros servicios los cuales son:

Tabla 9

Direcciones IP's relacionadas a los servicios evaluados

IP	Servicio	Numero de Paquetes	Porcentaje representativo en los datos capturados
172.16.0.98	BibliotecaVirtual	14042	3.3%

Estos servicios tienen encriptado todo el tráfico que gestionan, por lo que se genera una hipótesis que el servicio local que responde a la ip <172.16.0.98> no posee ningún certificado SSL que prevenga que antes que las peticiones a los repositorios externos sean capturadas sin ningún tipo de cifrado.

En el anexo de la prueba se podrá tener acceso a toda la trama de datos capturados en la prueba.

8.3. Prueba hombre en medio WhatsApp

Con el fin de verificar si una de las aplicaciones más utilizadas en las redes wifi-abiertas y siendo una herramienta de comunicación masiva elemental e importante para la mayoría de los usuarios, se realiza un ataque para verificar la seguridad de WhatsApp.

Se realizó un ataque de hombre en el medio usando como herramienta la suite airdump en Kali Linux, realizando una captura de paquetes durante 3 minutos únicamente sobre tráfico de entrada y de salida desde la aplicación de mensajería instantánea WhatsApp.

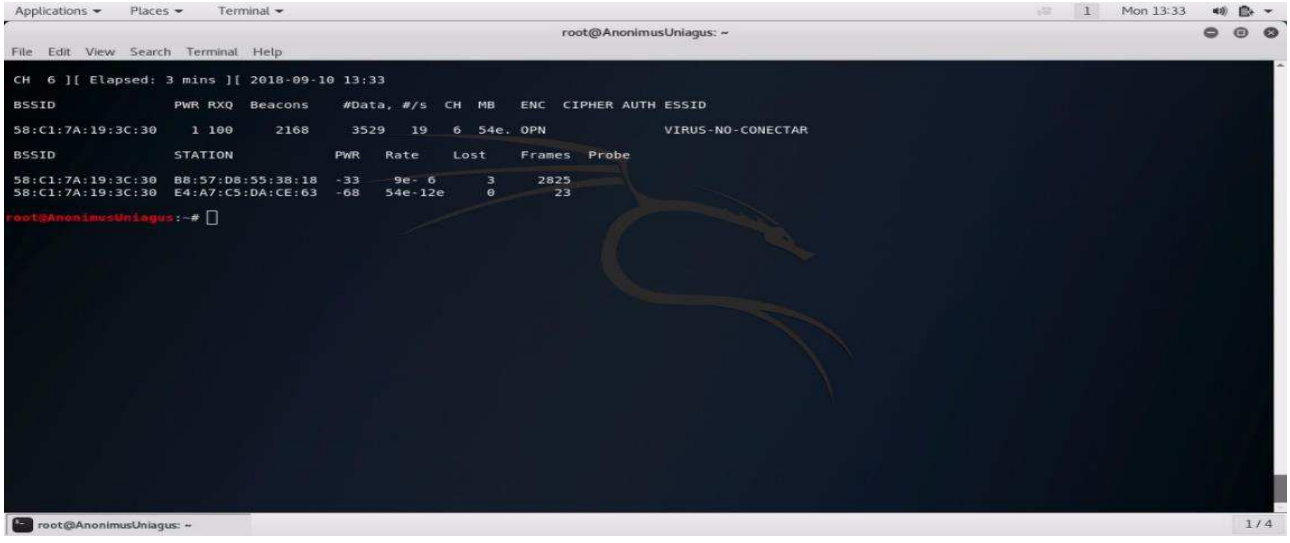

Figura 11 Proceso de captura de tráfico sobre SSID “VIRUS-NO-CONECTAR” para la aplicación WhatsApp.

Sobre el tráfico obtenido, se logra obtener tráfico de entrada y salida hacia una dirección ip publica desde el dispositivo en pruebas. Se encontró que la dirección ip publica 157.240.14.53 posee una ubicación en las coordenadas “37°27'32.4"N 122°10'41.2"W” ubicado en la ciudad de Menlo Park, California y asociado a Facebook Inc.

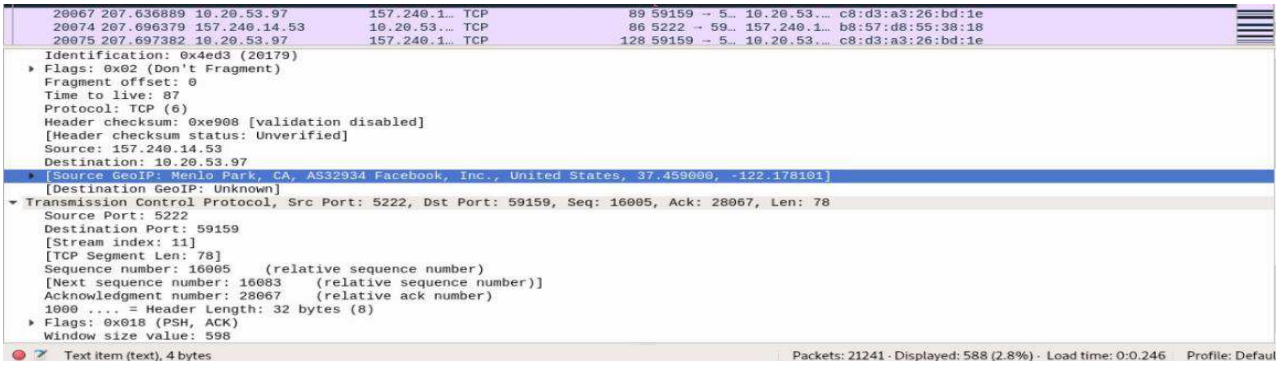

Figura 12 Valores geológicos de la dirección IP publica 157.240.14.53

Validando la información geológica de la ip obtenida, se encuentra que la dirección hace referencia a una zona residencial, por lo cual se tiene una hipótesis de que las peticiones las responde un servidor fantasma para así asegurar aún más la información del servidor.

Según la información compartida por WhatsApp en la web oficial acerca del cifrado en el documento "WhatsApp-Security-Withepaper" se comparte a la comunidad las 3 llaves públicas que son generadas al momento de la instalación de la aplicación (Identity Key Pair, Signed Pre Key, One-Time Pre Keys), y las tres llaves de sesión (Root Key, Chain Key, Message Key). (WhatsApp, 2017)

Analizando las capturas de tráfico tanto de entrada como de salida sobre la dirección ip publica, se encuentra que efectivamente toda la información se encuentra cifrada y sin indicios de poder hallar las claves públicas o en si el mensaje enviado.

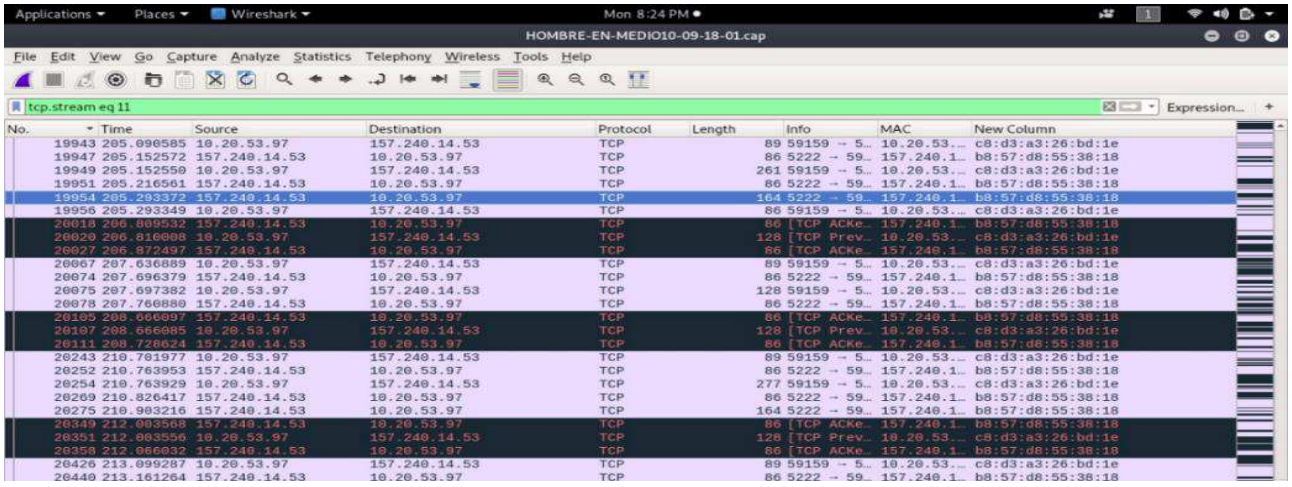

Figura 13 Trafico capturado desde la aplicación de WhatsApp

Figura 14 Trafico analizado desde la aplicación de WhatsApp

Efectivamente WhatsApp cifra el contenido desde que el mensaje es enviado, protege la ubicación física de sus servidores donde puede llegar a ser interceptado toda la información de sus usuarios. Aunque la información esté cifrada, si fue capturada una gran cantidad de tráfico (que puede ser revisada en el anexo de las pruebas realizadas) y dicho tráfico puede llegar a ser descifrado por algún individuo que posea un amplio conocimiento acerca de protocolos de encriptación.

8.4. Prueba hombre en medio Gmail App

El servicio de mensajería por medio de correo electro se ha establecido como uno de los medios de comunicación formal más usados en el mundo y la comunidad educativa no ha menospreciado esta valiosa herramienta. Mediante el uso de los correos institucionales por medio de la plataforma de correo electrónico Gmail, la universitaria agustiniana enfoca gran parte de la comunicación entre la institución y los estudiantes. Por este mismo motivo gran cantidad de información que puede llegar a ser sensible y es por este motivo que se realiza una prueba a la seguridad de la información de la plataforma de correos de Google.

Se realizó un ataque de hombre en el medio capturando todo el tráfico generado desde el aplicativo móvil de Gmail. Se capturaron un total de 25.348 paquetes de los cuales 3149 son relevantes y asociados al servicio de correo electrónico de Google.

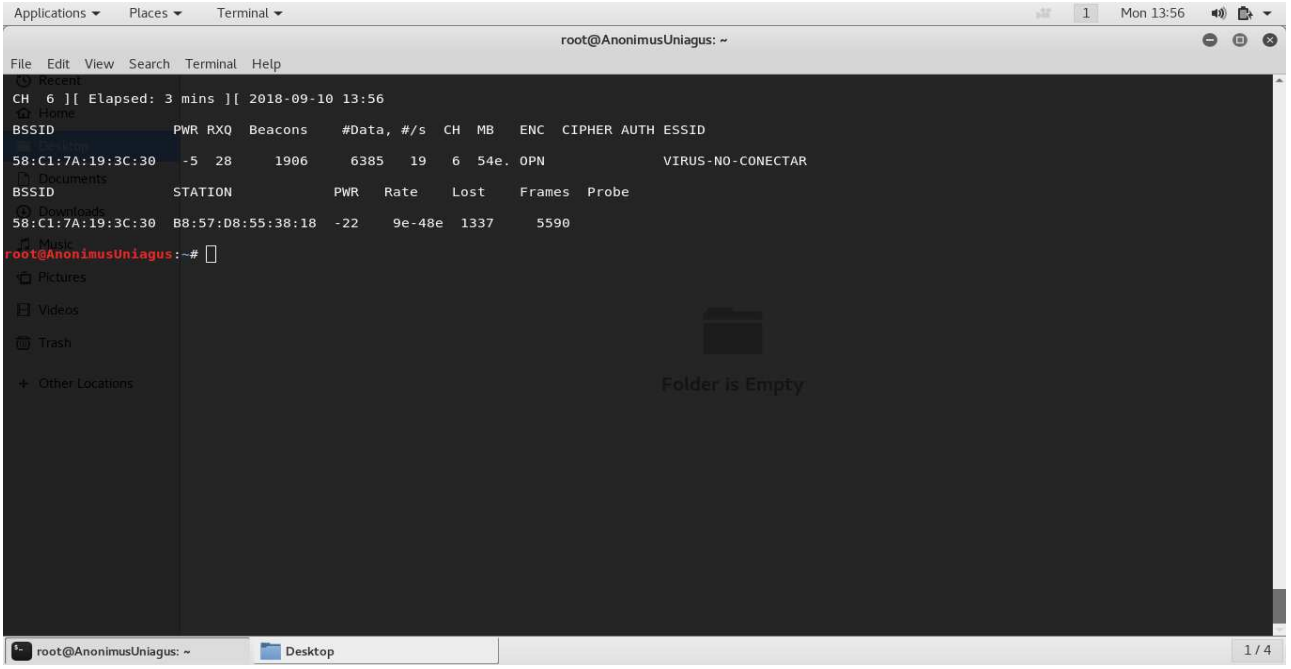

Figura 15 Proceso de captura de tráfico sobre SSID "VIRUS-NO-CONECTAR" para la aplicación WhatsApp

Los servidores en base a su ubicación responden a los laboratorios dentro del perímetro de la NASA.

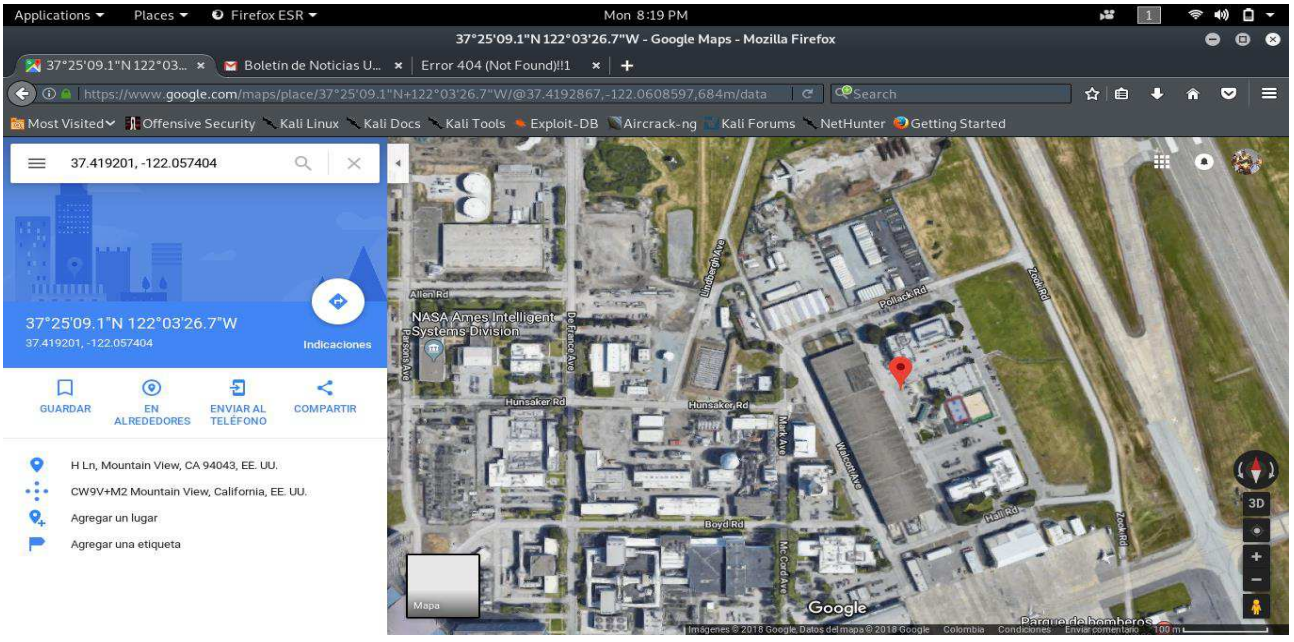

Figura 16 Ubicación geográfica de los servidores pertenecientes a servicios de Google.

Las direcciones IP más relevantes se encuentran descritas en la siguiente tabla.

Tabla 10

Cantidad de paquetes relevantes enviados y recibidos en la prueba del servicio Gmail

IP	Servicio	Número de Paquetes	Porcentaje representativo en los datos capturados
172.217.28.110	Google LLC	1288	5,1%
172.217.28.101	Google LLC	52	0,2%
172.217.28.109	Google LLC	741	2,9%
172.217.28.99	Google LLC	196	0,8%
216.58.222.202	Google LLC	872	3,4%

Se logró capturar 1288 paquetes desde la dirección IP 172.217.28.110 de los cuales el 100% se encuentra cifrado.

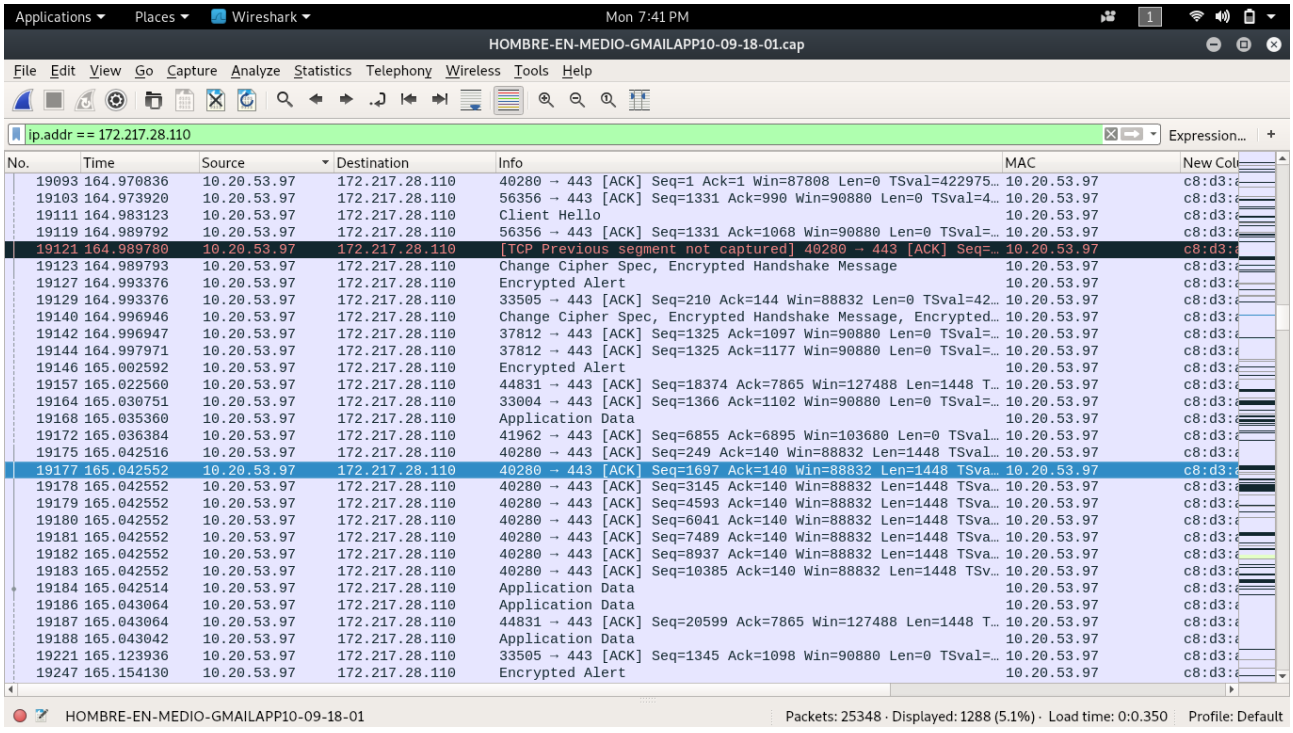

Figura 17 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.110

Se encuentra que la IP corresponde a servicios de Google por los valores hallados en la Geolocalización del parámetro IPV4

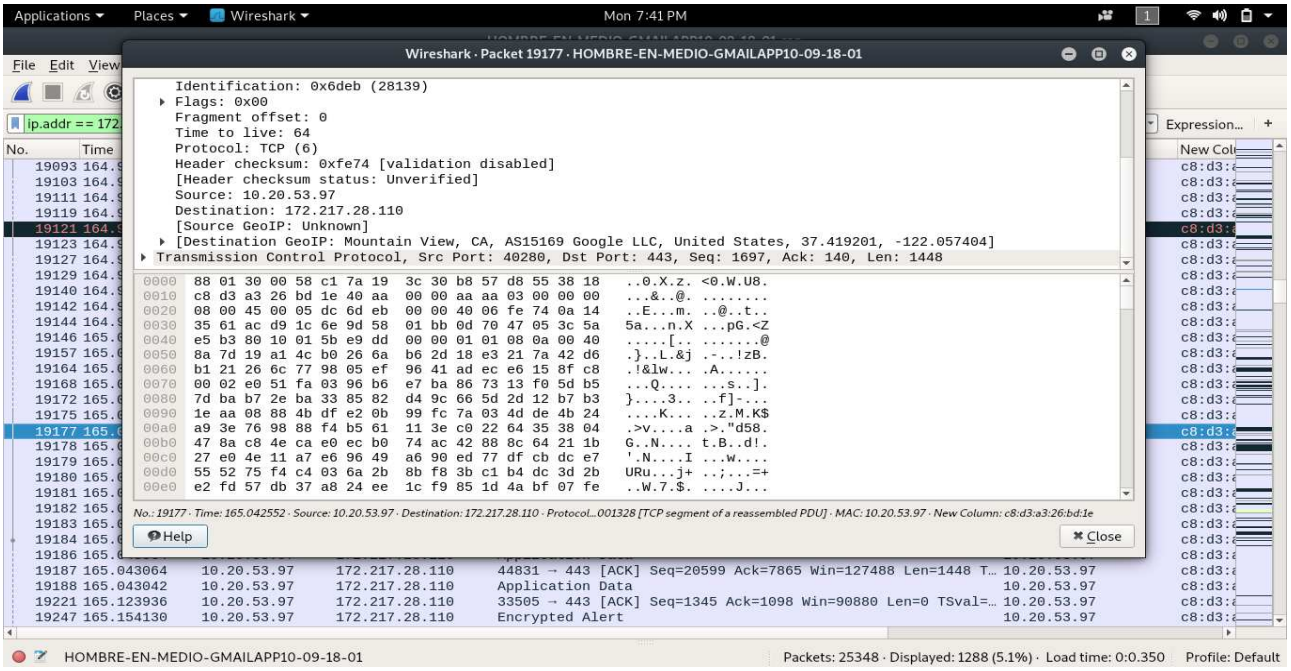

Figura 19 Valores de geolocalización e identificación de la dirección IP 172.217.28.110

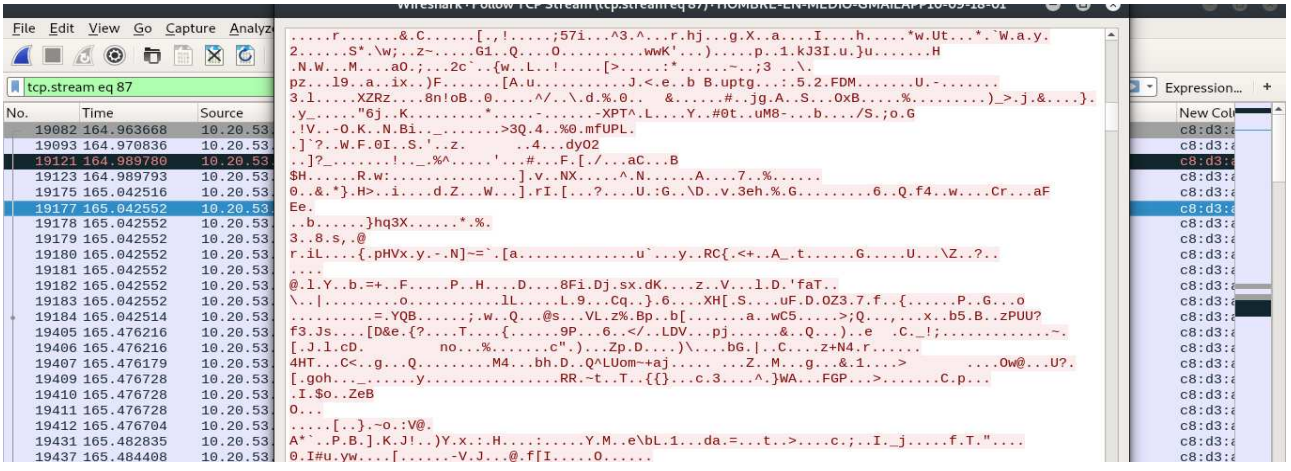

Figura 18 Paquete analizado proveniente de los servicios de Google

Para la dirección IP 172.217.28.101 se capturaron 52 paquetes, de los cuales todos se encuentran cifrados.

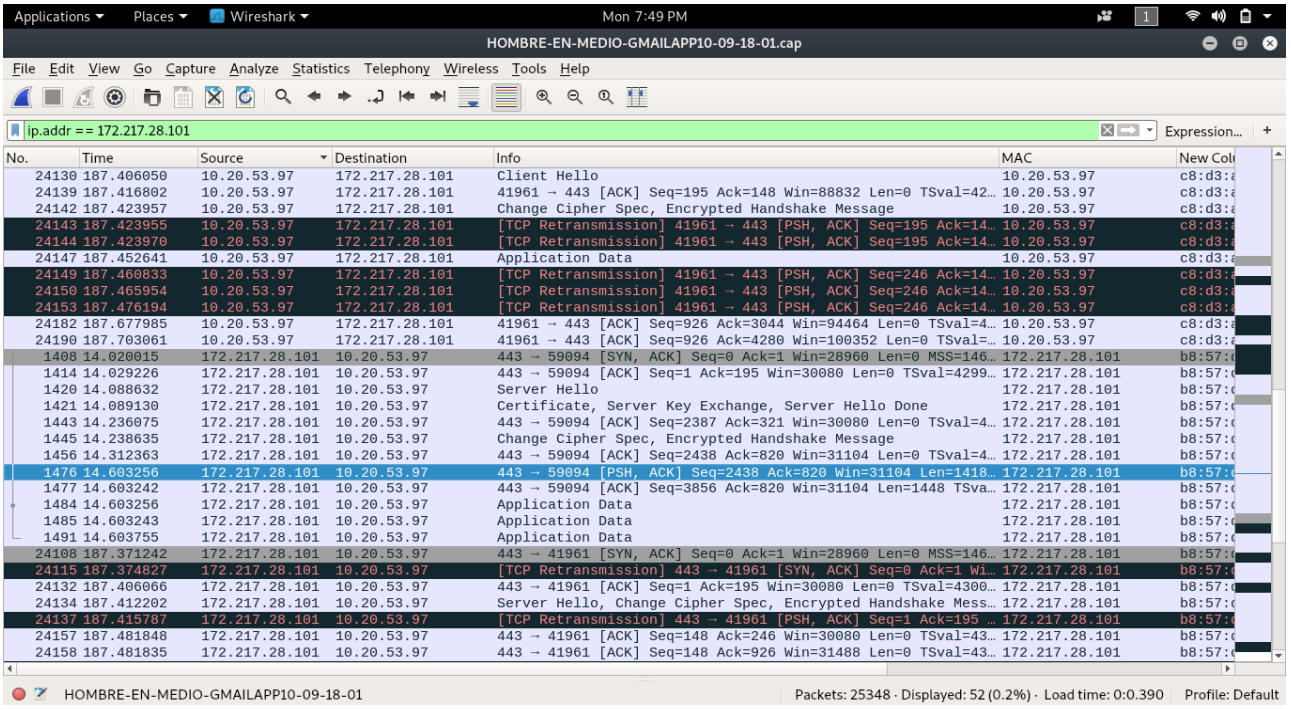

Figura 20 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.101

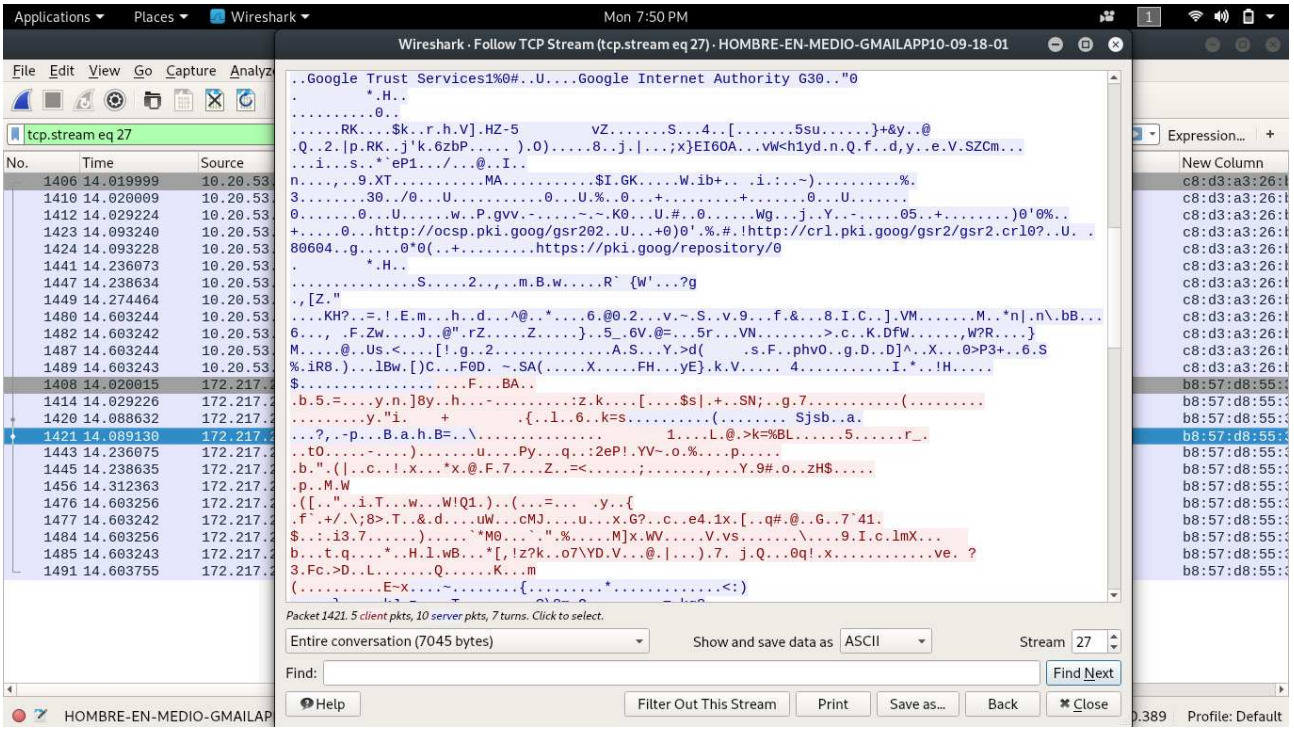

Figura 21 Paquete analizado proveniente de la dirección IP 172.217.28.101

Se concluye que proviene de un servicio de Google por el contenido de las URL visibles dentro de los paquetes capturados y por los parámetros de geolocalización del protocolo IPV4

Se capturaron un total de 741 paquetes con relación a la dirección IP 172.217.28.109 de los cuales el 100% se encuentra cifrado.

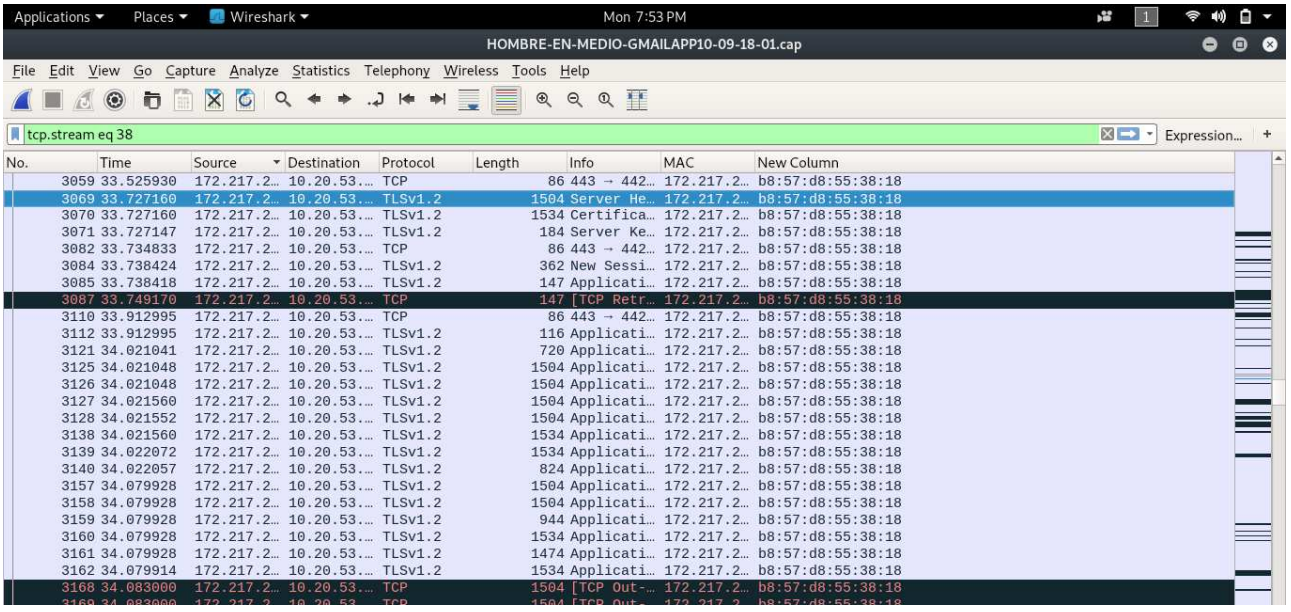

Figura 23 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.109

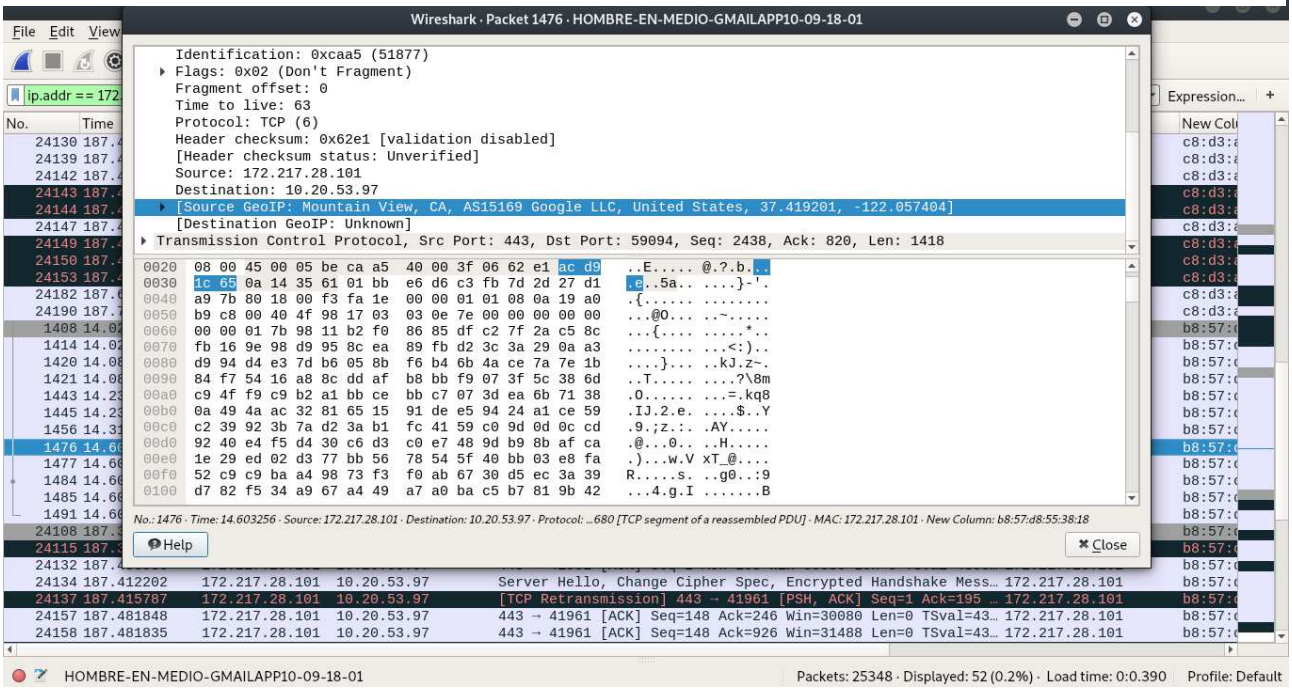

Figura 22 Valores de geolocalización e identificación de la dirección IP 172.217.28.101

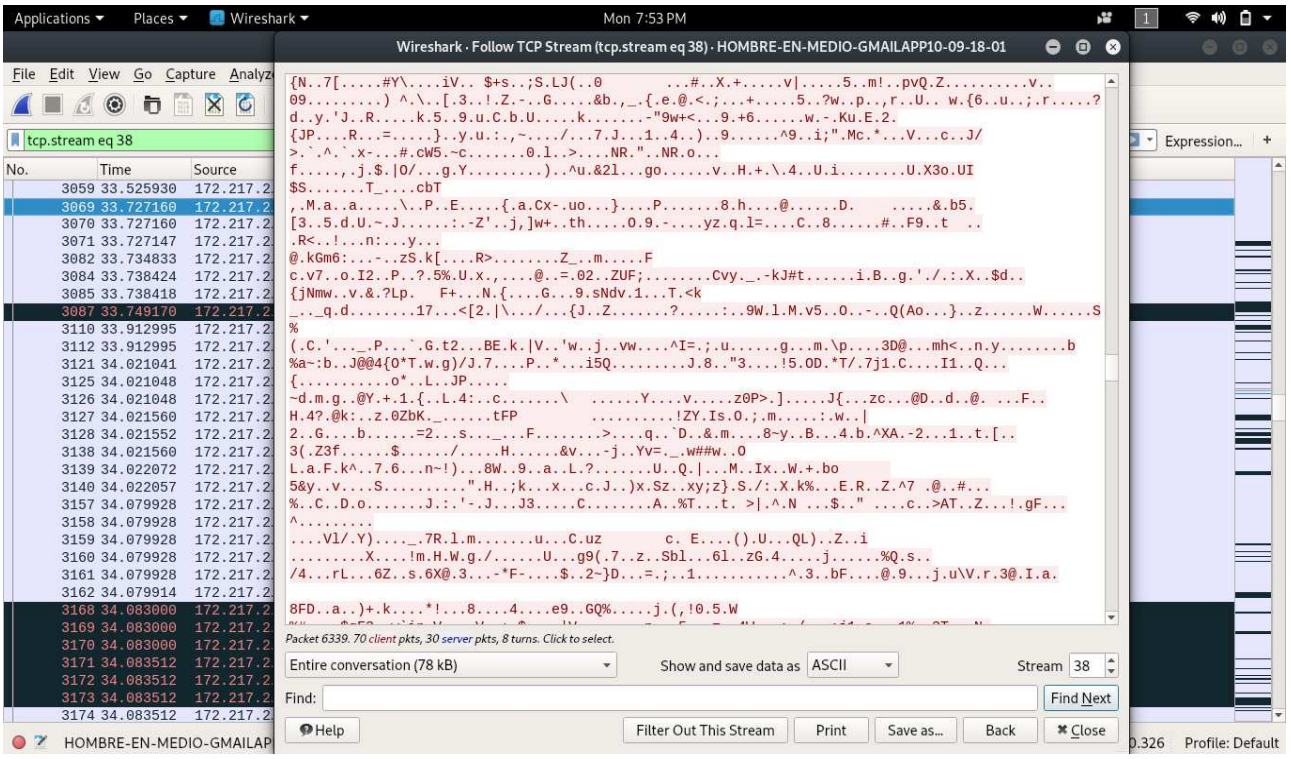

Figura 24 Paquetes analizados proveniente de la dirección IP 172.217.28.109

Se asocia con servicio de Google por los valores de geolocalización y algunas URL's visibles en algunos encabezados de los paquetes.

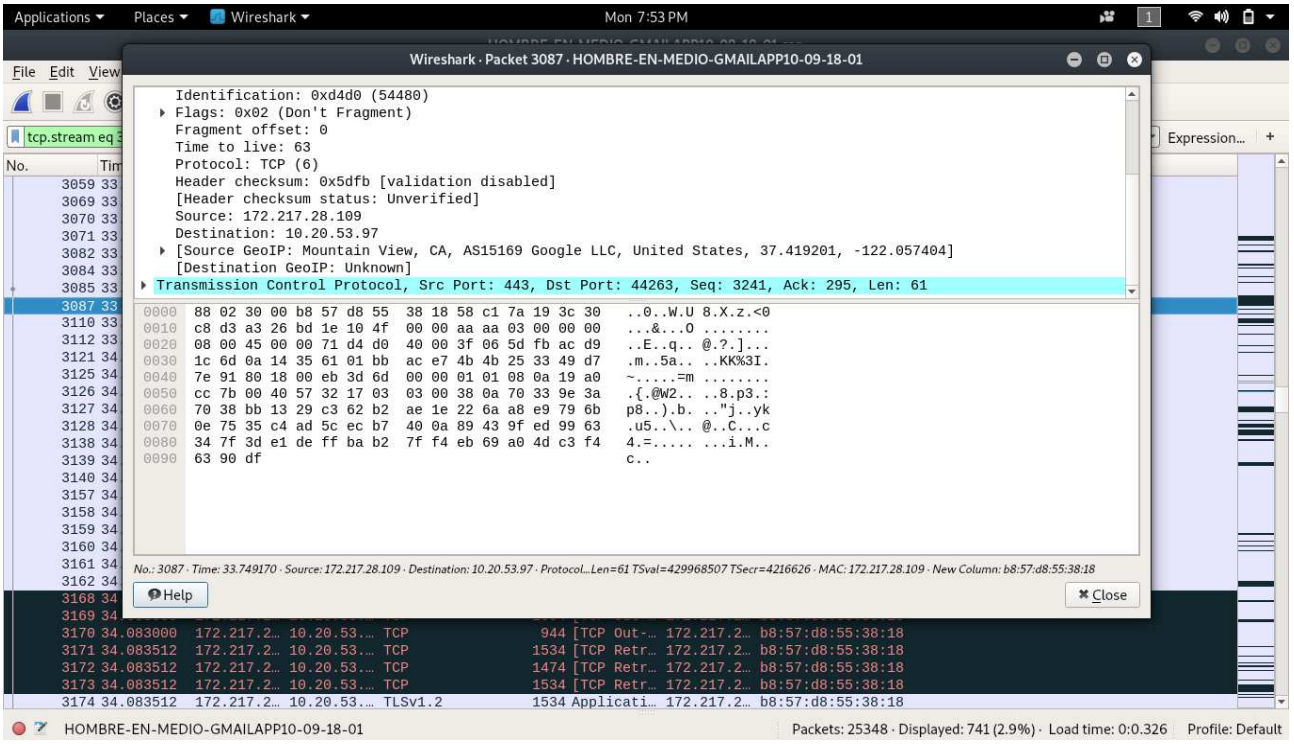

Figura 25 Valores de geolocalización e identificación de la dirección IP 172.217.28.109

La dirección IP 172.217.28.99 envió y recibió un total de 196 paquetes de los cuales el 100% está encriptado.

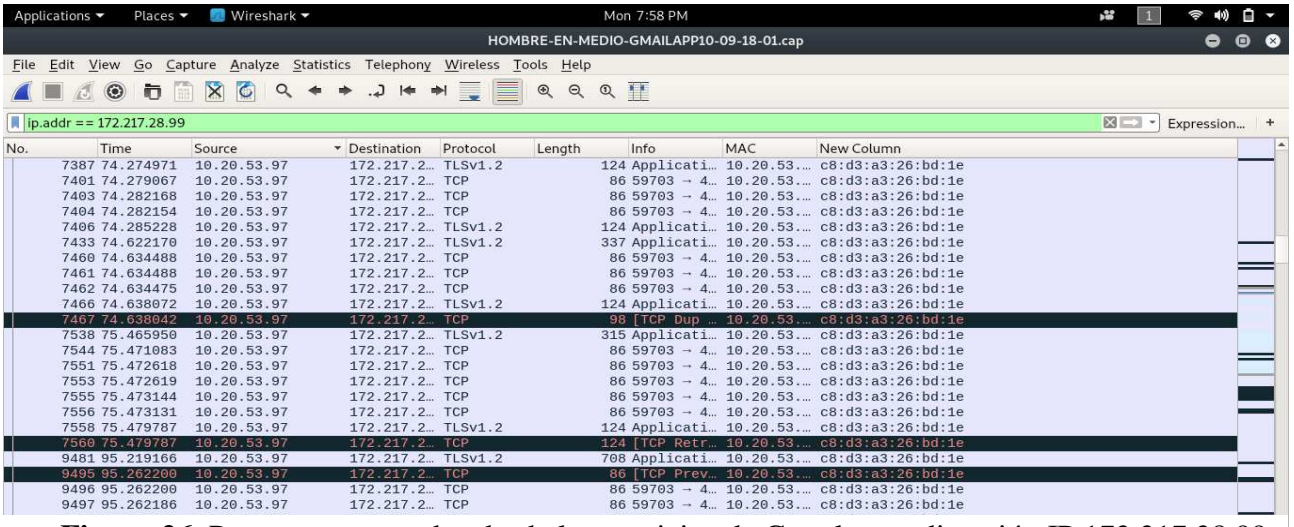

Figura 26 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.99

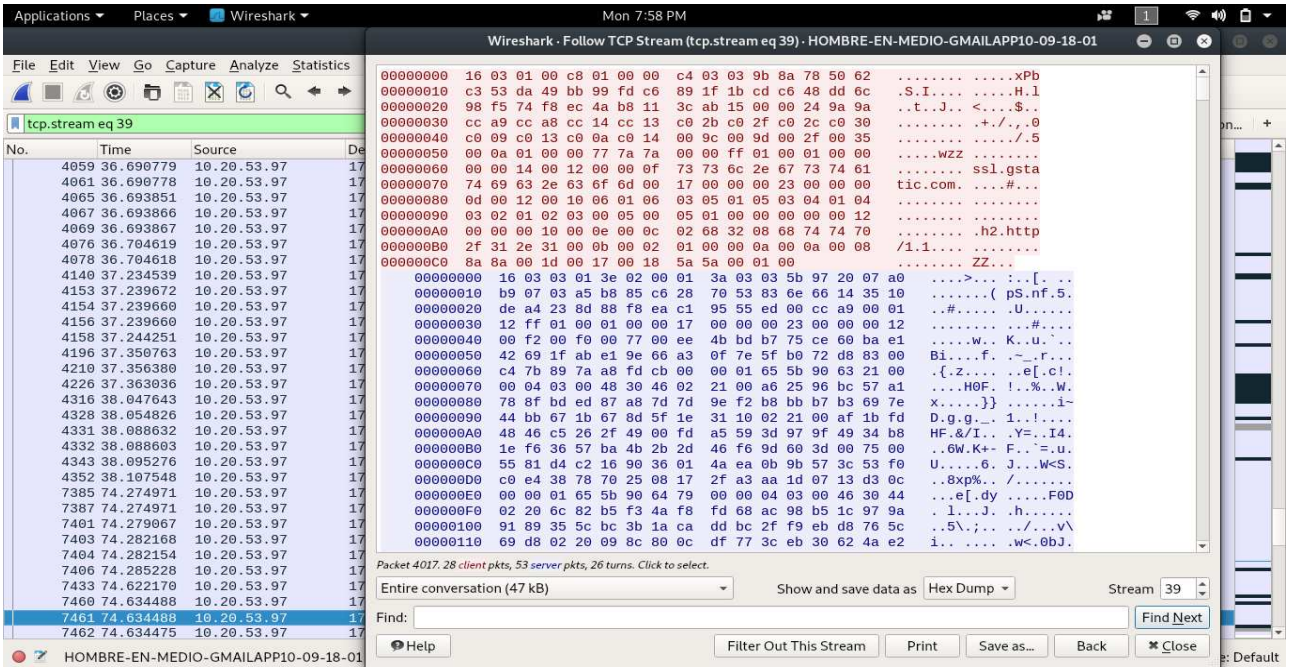

Figura 27 Paquetes analizados provenientes desde la dirección IP 172.217.28.99

Se asocia con un servicio nativo de Google por los valores de geolocalización sobre la IP y algunas URL visibles en encabezados de paquetes

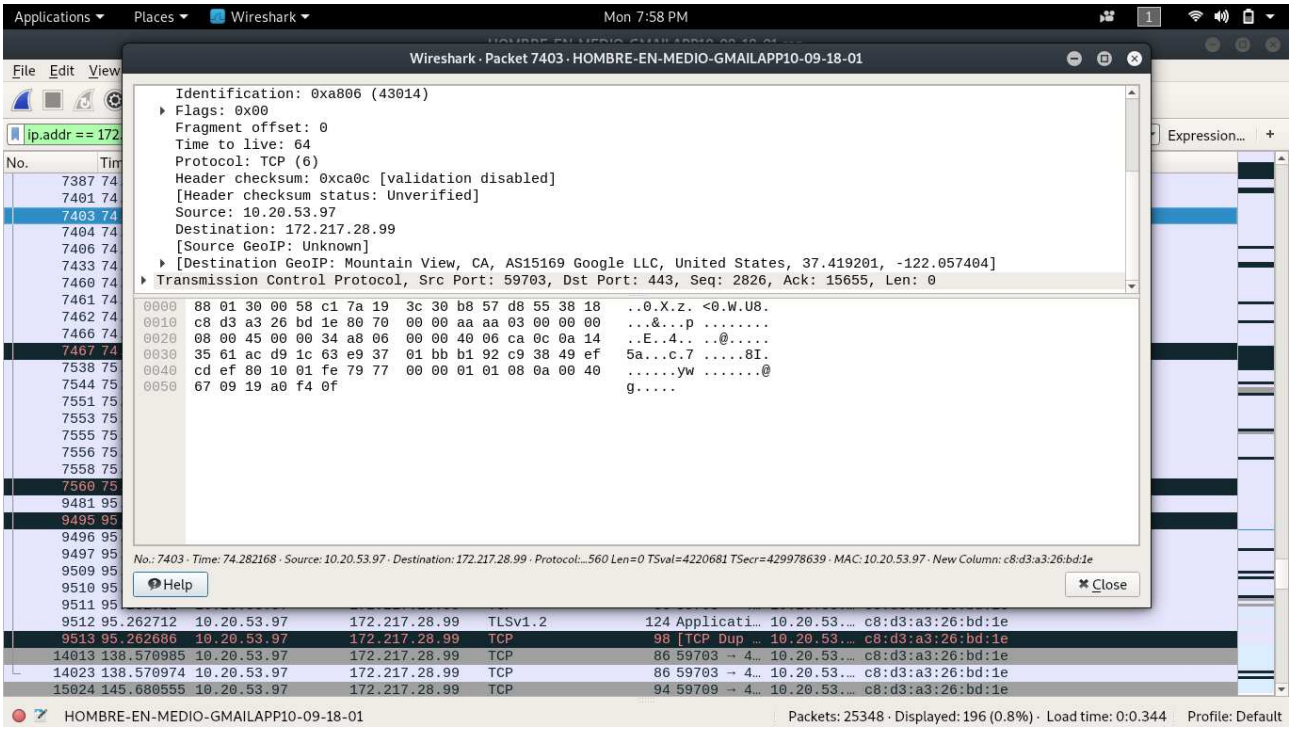

Figura 28 Paquetes capturados desde los servicios de Google y su geolocalización

La IP 216.58.222.202 que se encuentra un rango de direcciones totalmente diferentes a las demás, generó un total de 872 paquetes donde su totalidad están cifrados.

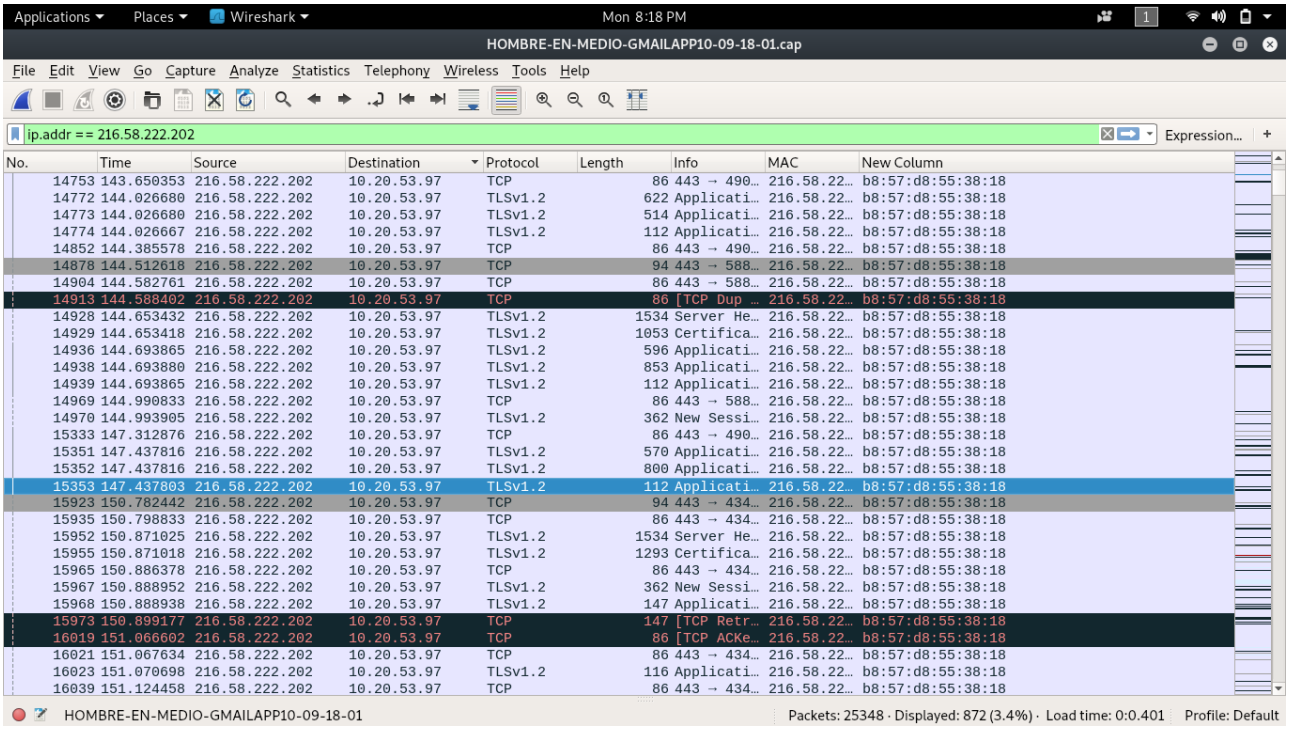

Figura 29 Paquetes capturados con dirección IP 216.58.222.202

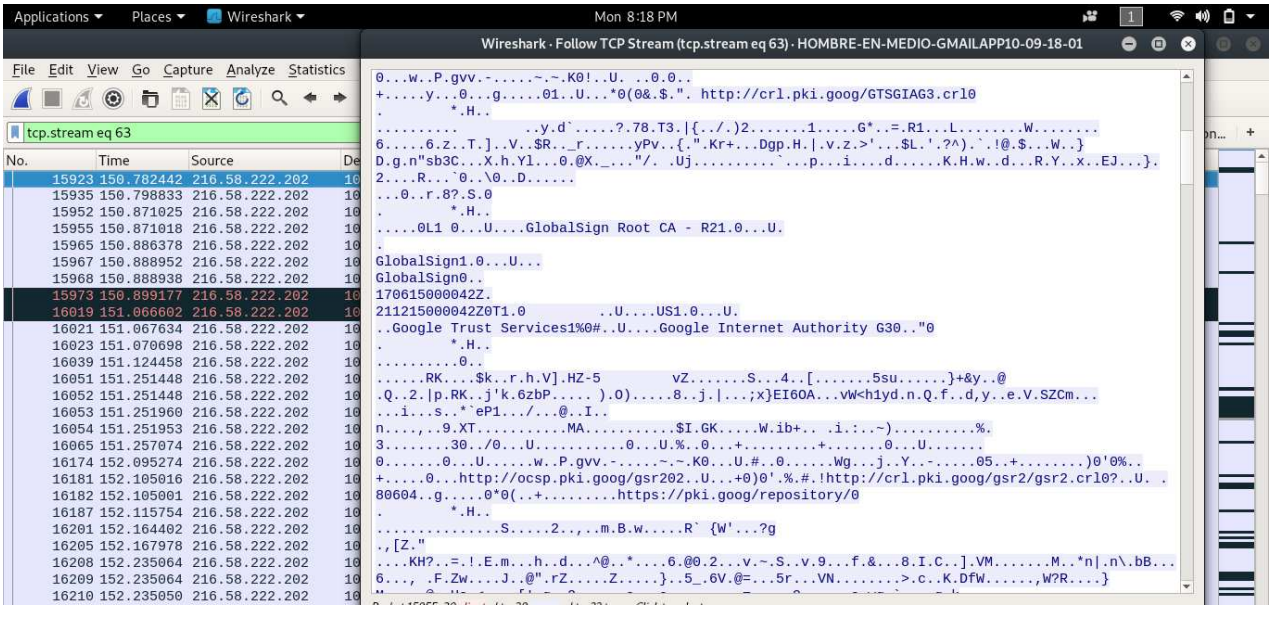

Figura 30 Evidencia de trafico cifrado desde la dirección IP 216.58.222.202

Se asocia a un servicio de Google, por las URL´s en los encabezados de los paquetes, y los valores encontrados dentro de los parámetros de geolocalización del protocolo IPV4

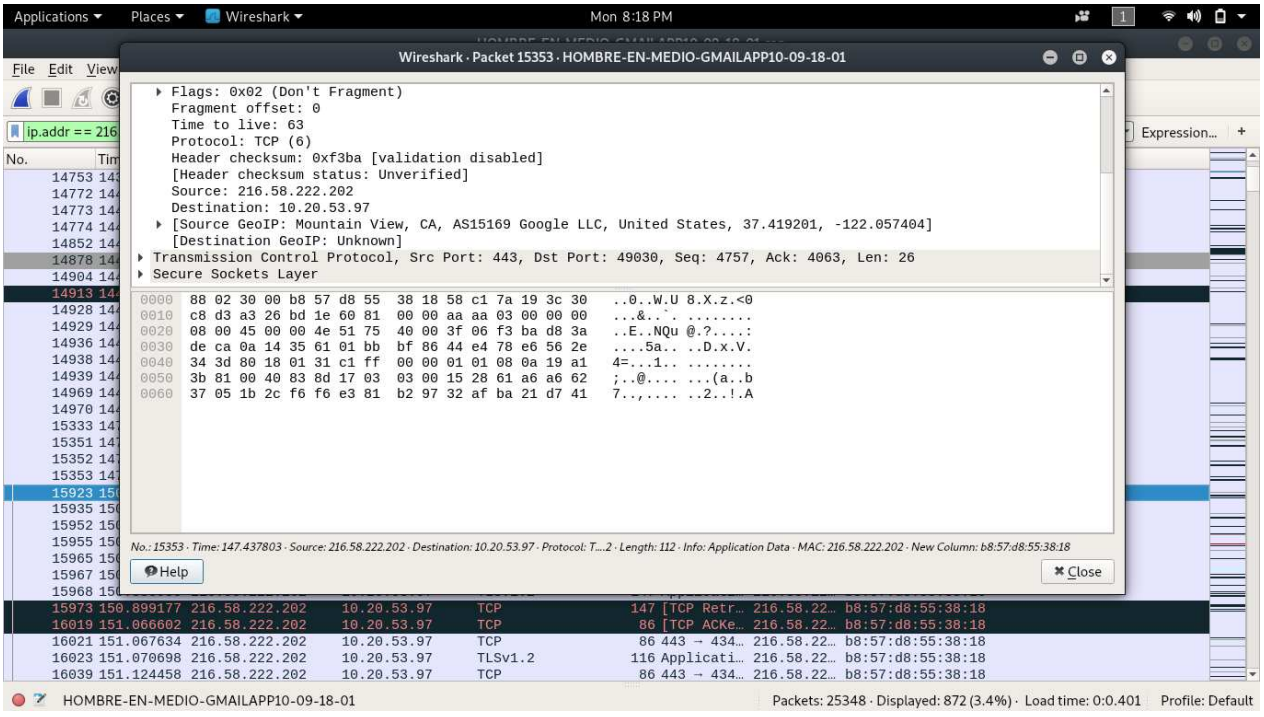

Figura 31 Paquetes capturados desde los servidores de Google con su geolocalización en protocolo IPV4

Efectivamente toda la información enviada, recibida y alojada dentro de los servicios de mensajería de Gmail son seguros y son enviados de manera encriptada desde el aplicativo móvil. Esto no hace que sea completamente seguro puesto que la información fue capturada, más sin embargo no es legible, dando una posibilidad a poder ser descifrada e interpretada.

8.5 Prueba hombre en medio Facebook

Facebook al ser la red social con más actividad por minuto la cual últimamente se ha visto involucrada en grandes escándalos de seguridad puesto que maneja grandes cantidades de información sensible de los usuarios. En este orden de ideas, se realiza una prueba de captura de información sobre una red WiFi abierta para verificar si efectivamente protege a sus usuarios.

Se realizó un ataque de hombre en el medio usando la suite airdump capturando tráfico generado desde el aplicativo de Facebook por medio de una red wifi abierta de nombre “VIRUS-NO-CONECTAR” realizada en un ambiente controlado.

Se lograron capturar un total de 45.868 paquetes, de los cuales únicamente 6834 paquetes relevantes. Dichos paquetes responden a las siguientes IP’s que influyen, actúan, o generan cierta relevancia dentro del tráfico generado.

Las IP´s públicas se describen en la siguiente tabla con el respectivo número de paquetes y su correspondiente porcentaje.

Tabla 11

Numero de paquetes relevantes para las pruebas del aplicativo de Facebook

IP	Servicio	Número de Paquetes	Porcentaje representativo en los datos capturados
31.13.65.7	Facebook	22	0,047%
31.13.65.38	Facebook Ireland	64	0,1%
157.240.6.23	Facebook	356	0,8%
157.240.6.18	Facebook	256	0,6%
157.240.6.19	Facebook	313	0,7%
200.114.57.81	EPM Telecomunicaciones	1122	2,4%
200.114.57.82	EPM Telecomunicaciones	1304	2,80%
186.31.253.81	IP BOGOTA COLOMBIA	3397	7,40%

Se encuentra que 4 IP´s de servidores provenientes de Facebook son las encargadas de responder las peticiones del servicio, sin embargo, estas IP´s manejan el mismo sistema de seguridad que los servidores de WhatsApp creando servidores fantasmas que respondan y reenvíen las solicitudes, ya que revisando la geolocalización que responde a estos, se encuentra una zona residencial. Esto sucede tanto con los ubicados en el condado de Menlo Park y en Dublín, Irlanda.

Efectivamente todo el tráfico generado usando la mayoría de las funcionalidades disponibles en la aplicación de Facebook, están cifrando la información y protegiéndola de que sea interceptada e

interpretada. Esto no la hace completamente segura, ya que, con conocimientos avanzados en cifrado, se podría leer toda la información capturada

Realizando un análisis al tráfico de entra y salida hacia cada una de las IP's generadas anteriormente, se encuentra lo siguiente.

El servicio de facebook que responde a la ip 31.13.65.7 donde se evidencia todo el tráfico enviado y recibido desde esta ip. Dicho tráfico está cifrado.

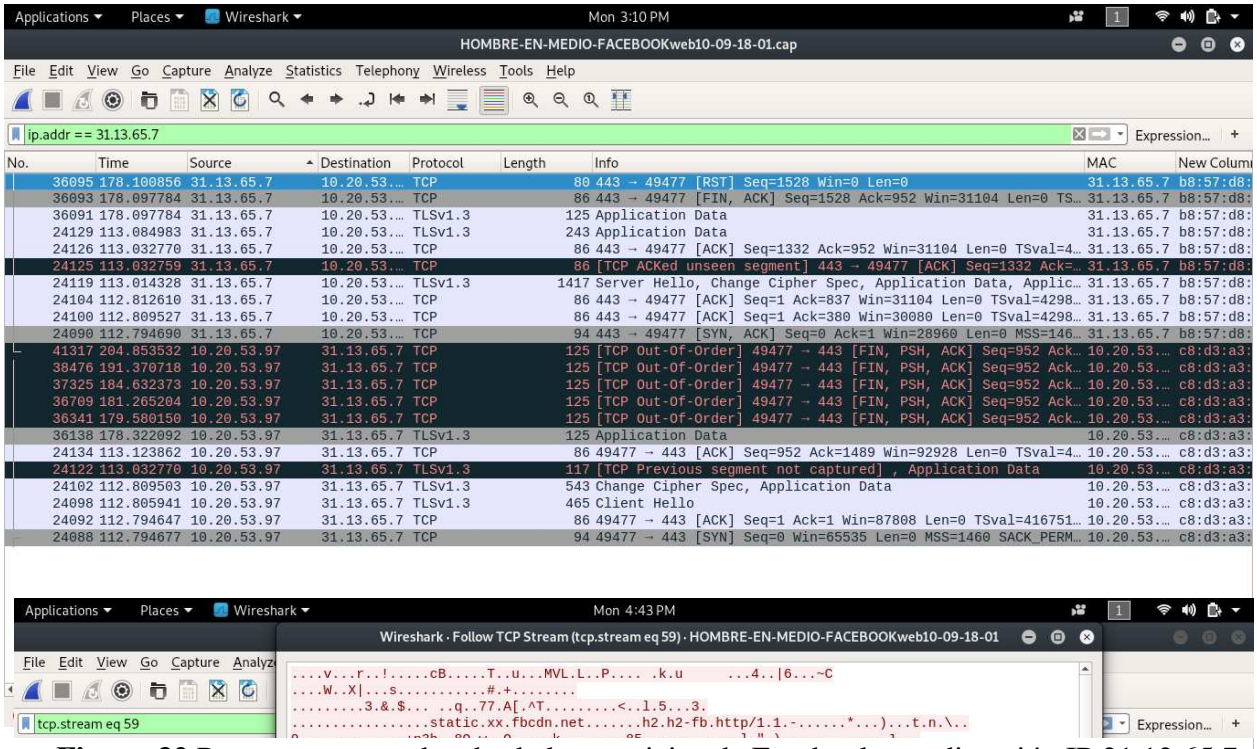

Figura 32 Paquetes capturados desde los servicios de Facebook con dirección IP 31.13.65.7

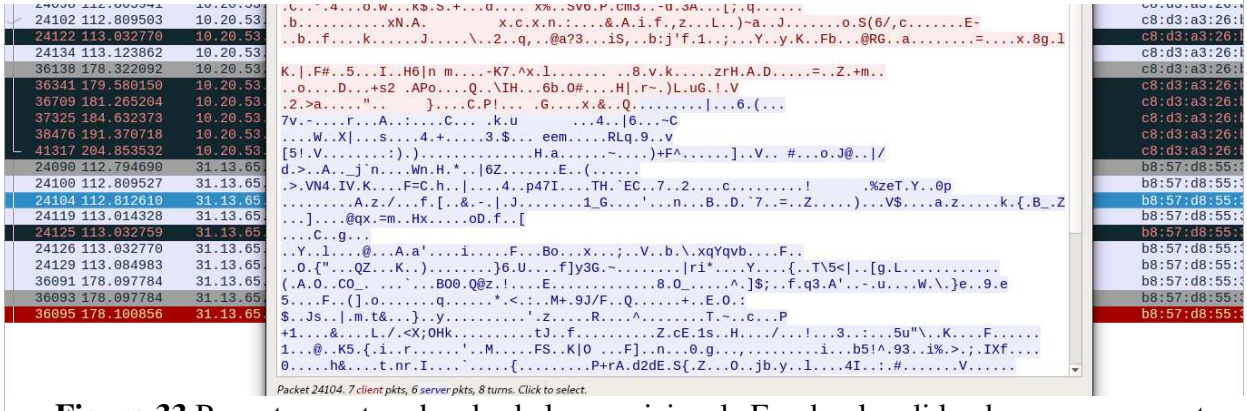

Figura 33 Paquetes capturados desde los servicios de Facebook validando que se encuentra la información encriptada.

Se reconoce que la dirección IP está asociada a Facebook por la geoip visualizada en los parámetros IPV4

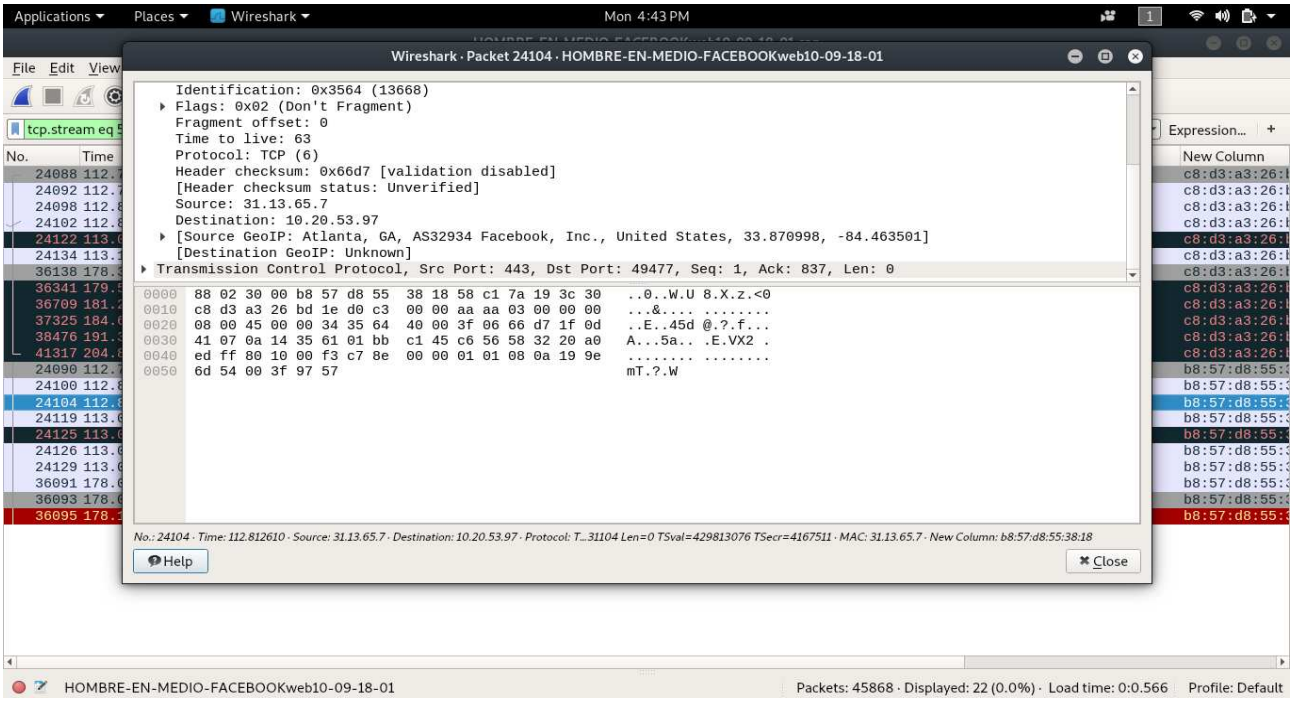

Figura 34 Paquetes capturados desde los servicios de Facebook con su geolocalización

El servicio de Facebook que responde a la dirección IP 31.13.65.38 donde se logra evidenciar que todo el tráfico generado desde y hacia dicha dirección IP está completamente cifrado.

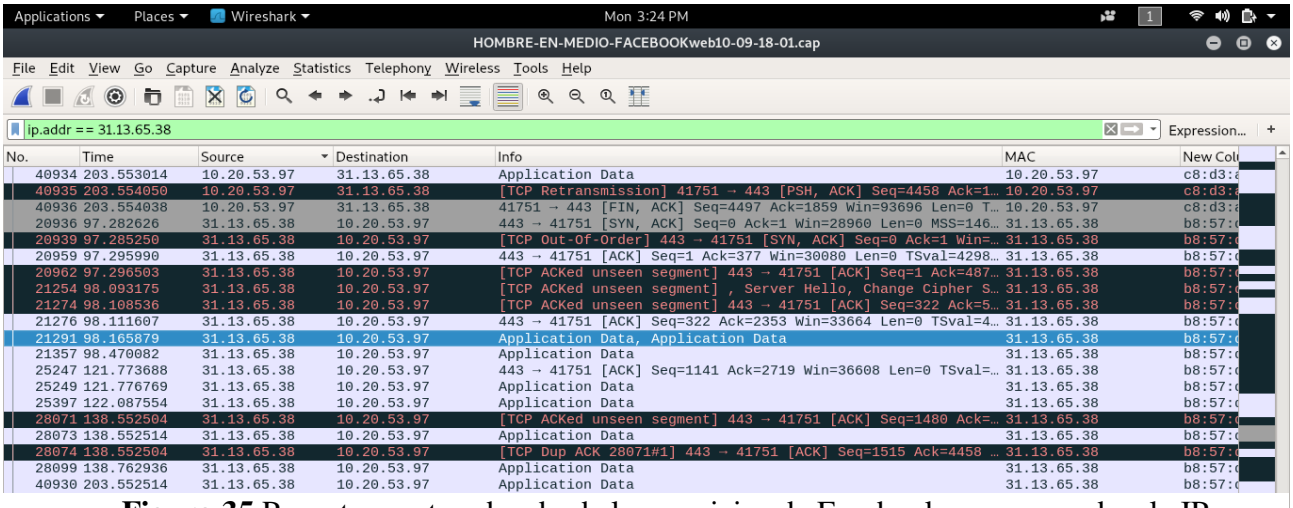

Figura 35 Paquetes capturados desde los servicios de Facebook que responde a la IP 31.13.65.38