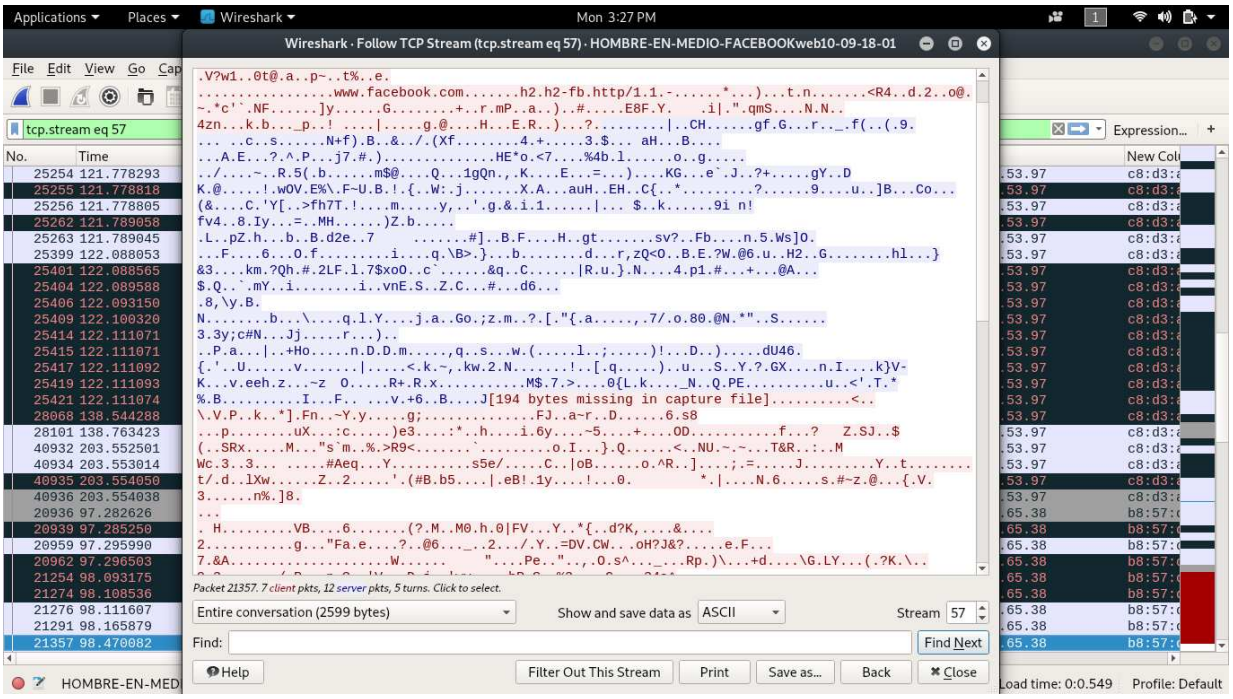

Figura 36 Paquetes capturados desde los servicios de Facebook

Se sabe que dicha ip responde desde Facebook por los valores de geoip hallados en el apartado de IPV4.

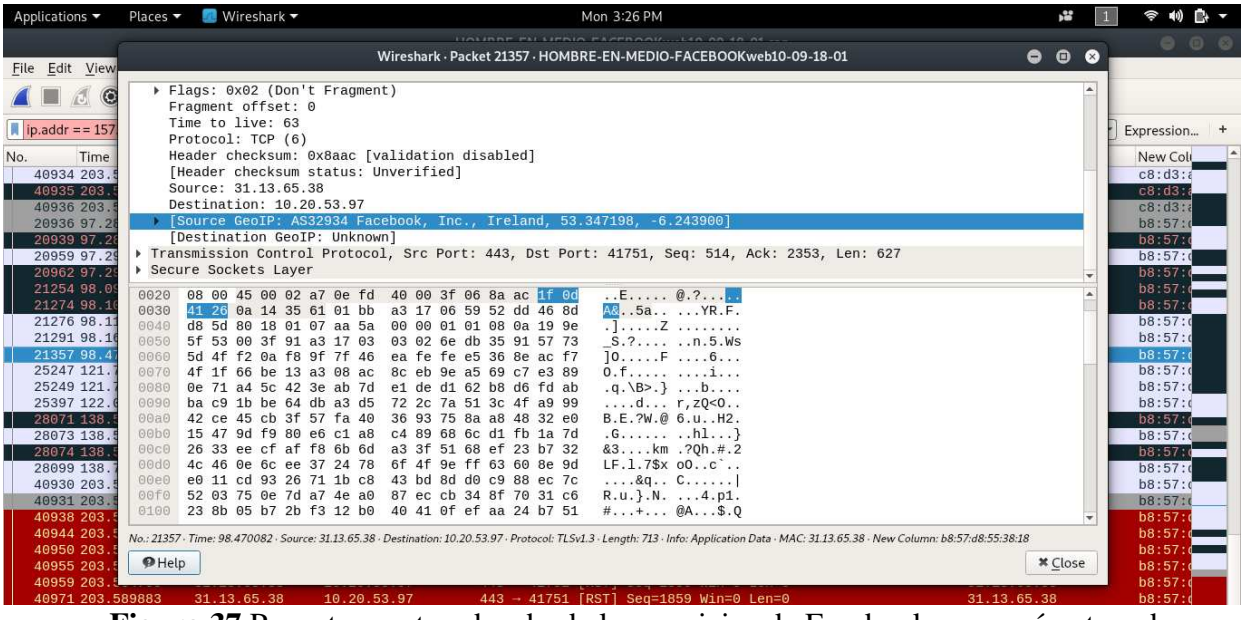

Figura 37 Paquetes capturados desde los servicios de Facebook con parámetros de geolocalización.

Los servicios de Facebook más representativos en dicha captura son los asociados a las direcciones IP's <157.240.6.23; 157.240.6.18; 157.240.6.19> las cuales completan la mayor parte de paquetes

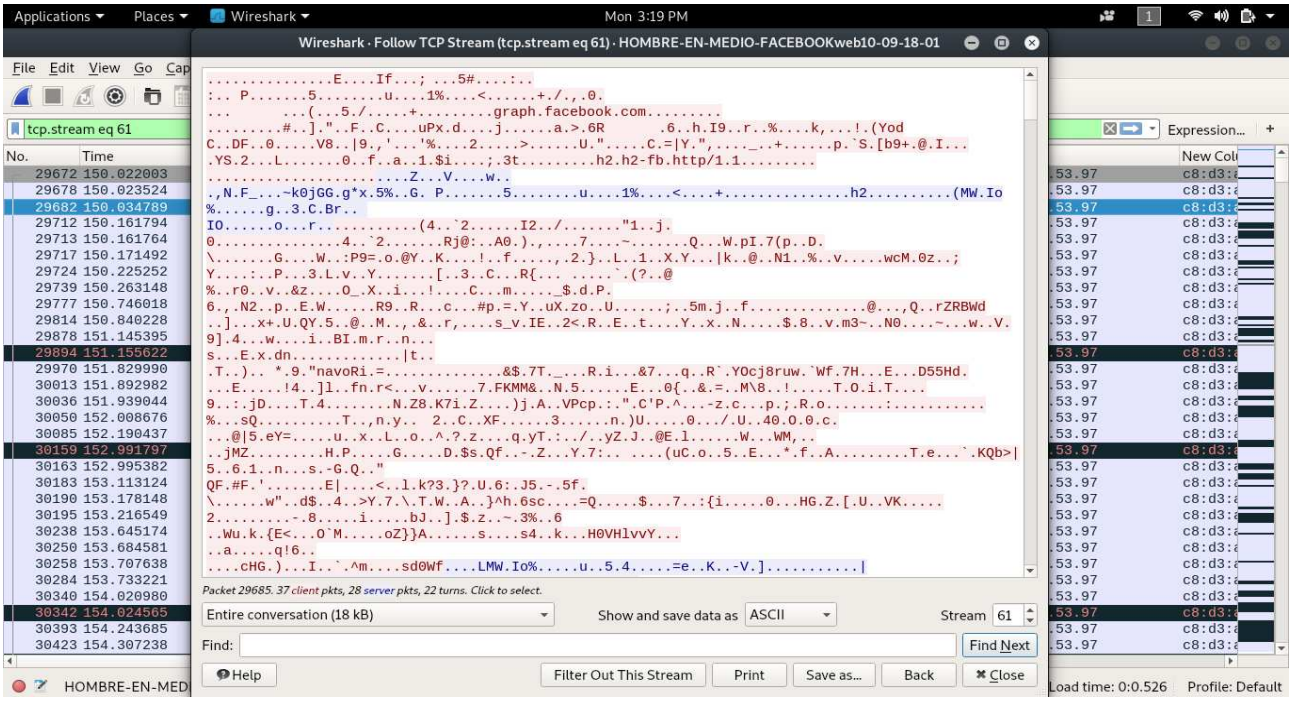

Figura 38 Paquetes capturados desde los servicios de Facebook evidenciando su total encriptación

provenientes de Facebook con un total de 925, de los cuales el 100% está completamente cifrado.

Para la ip 157.240.6.18, se capturan un total de 256 paquetes de los cuales están completamente cifrados.

Como en los casos anteriores, se encuentra que pertenece a Facebook por los valores de geoip en el parámetro IPV4

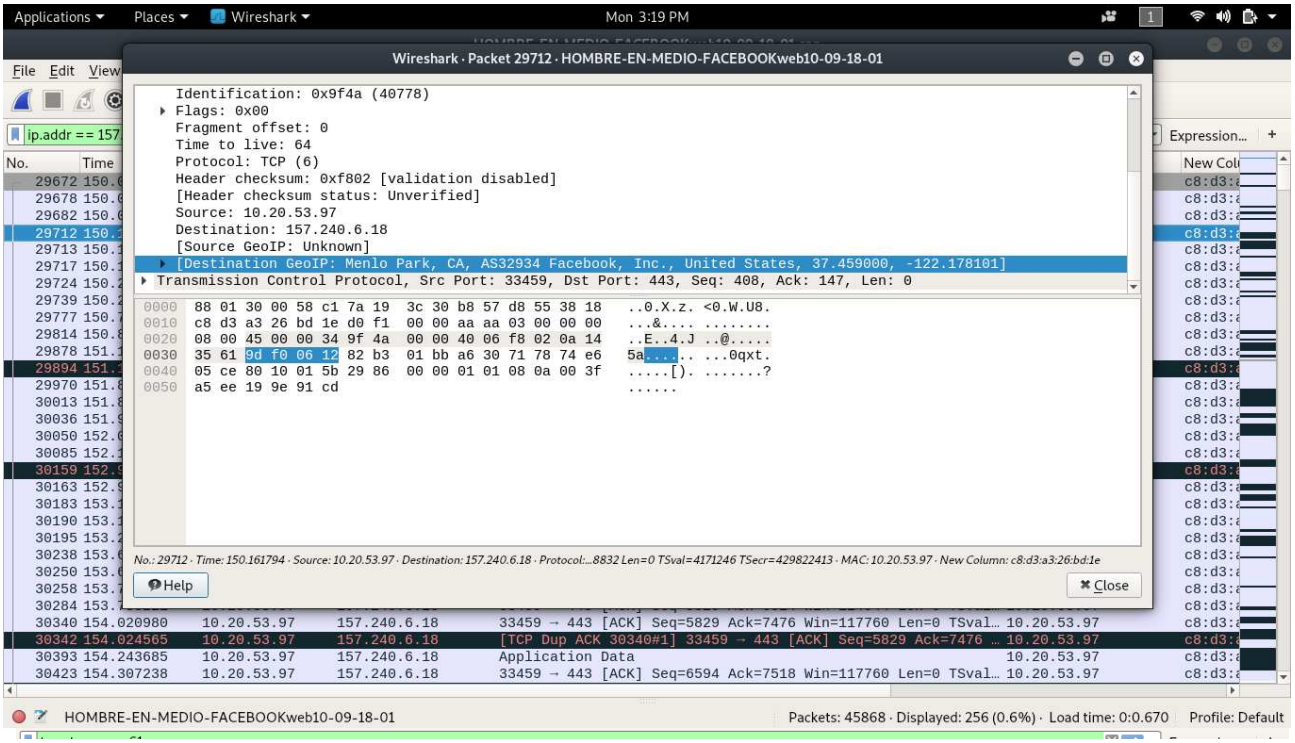

Figura 40 Paquetes capturados desde los servicios de Facebook con valores de GeoIP

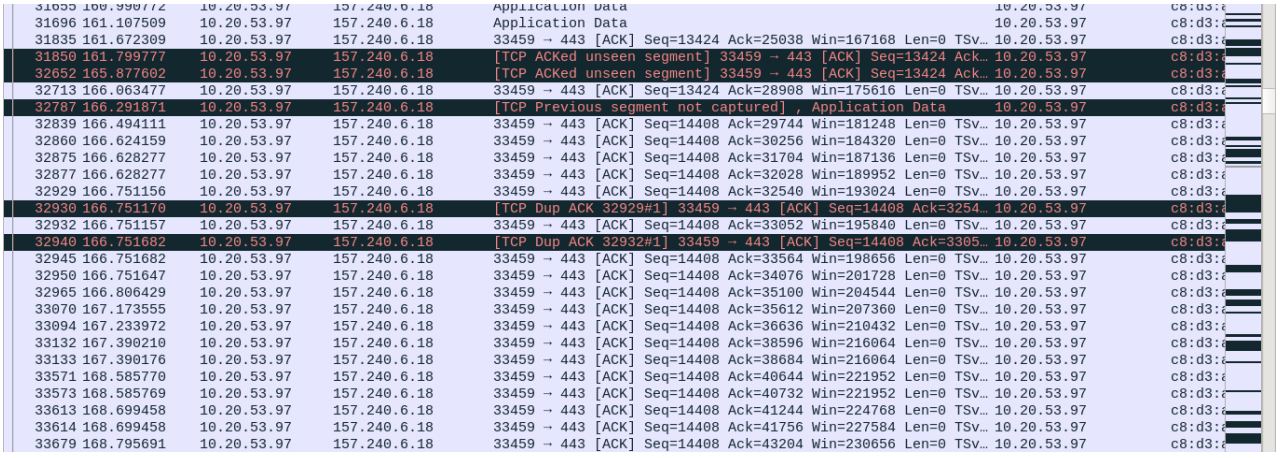

Figura 39 Paquetes capturados desde los servicios de Facebook respondiendo a la IP 157.240.6.18

Para la ip 157.240.6.19, se capturan un total de 313 paquetes de los cuales están completamente cifrados.

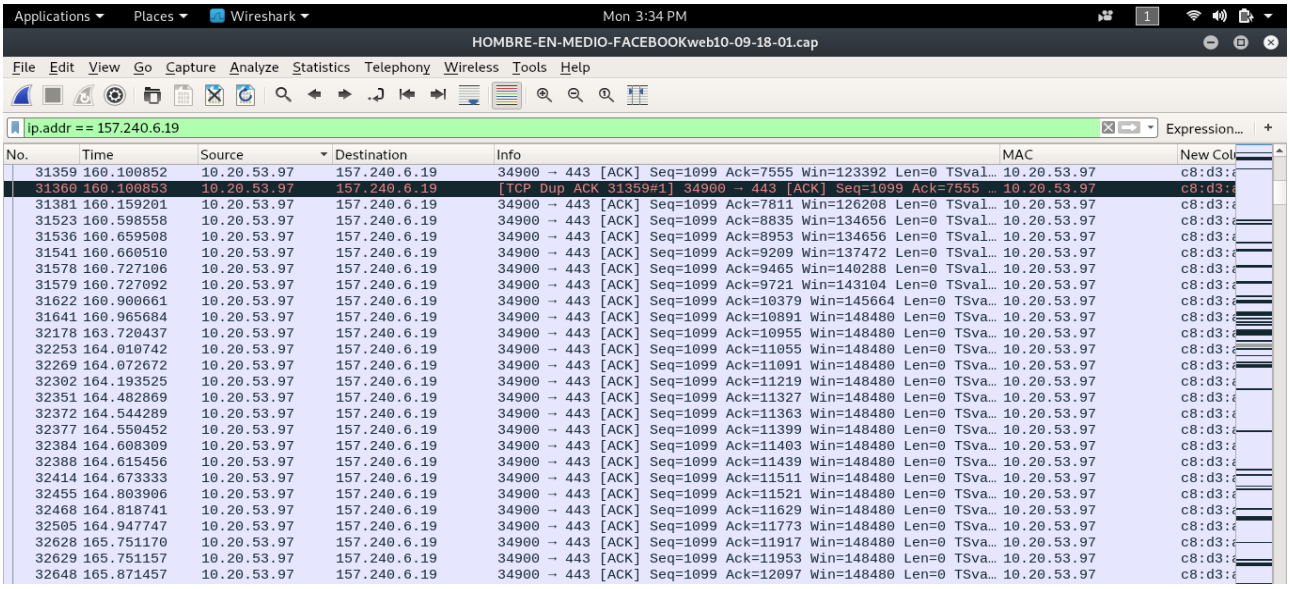

Figura 41 Paquetes capturados desde los servicios de Facebook

Se encuentra que pertenece a Facebook por los valores de geoip en el parámetro IPV4

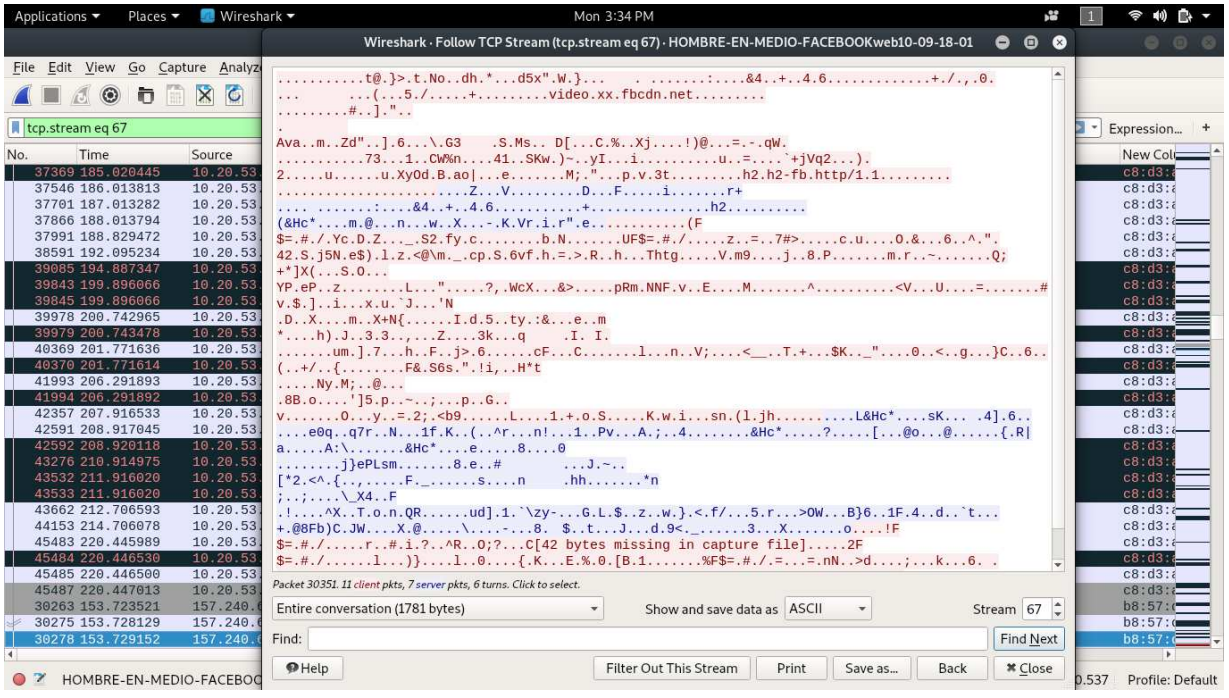

Figura 42 Paquetes capturados desde los servicios de Facebook evidenciando su cifrado

Para la ip 157.240.6.23, se capturan un total de 356 paquetes de los cuales están completamente cifrados.

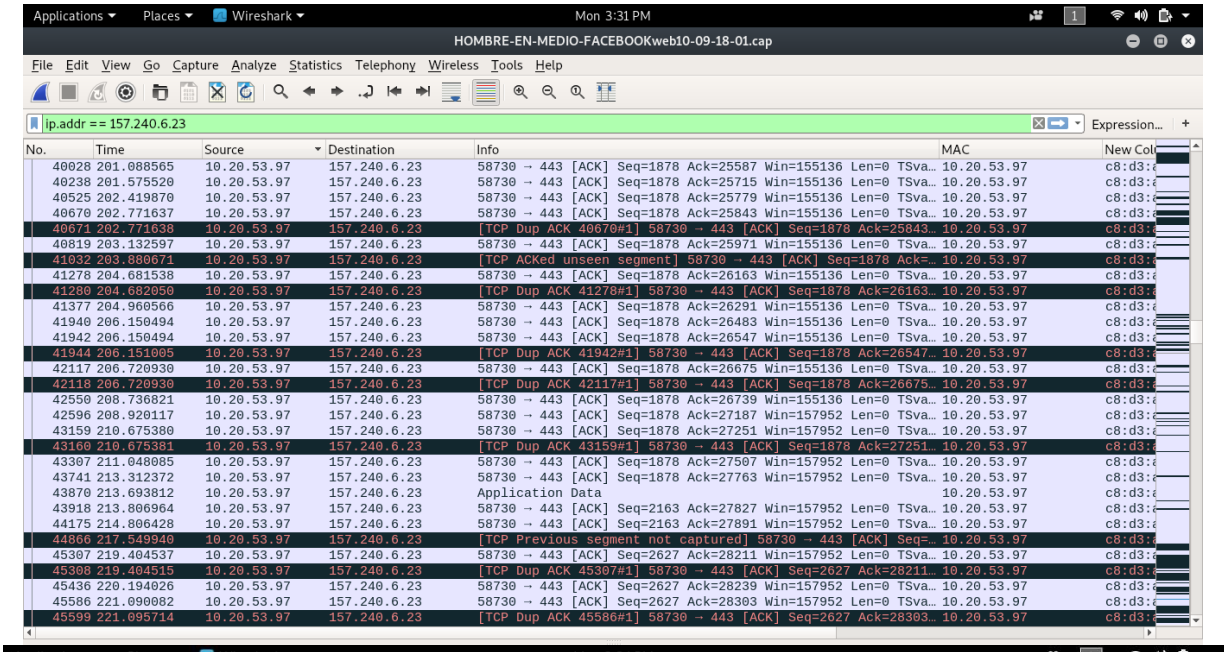

Figura 44 Paquetes capturados desde los servicios de Facebook respondiendo a la IP 157.240.6.23

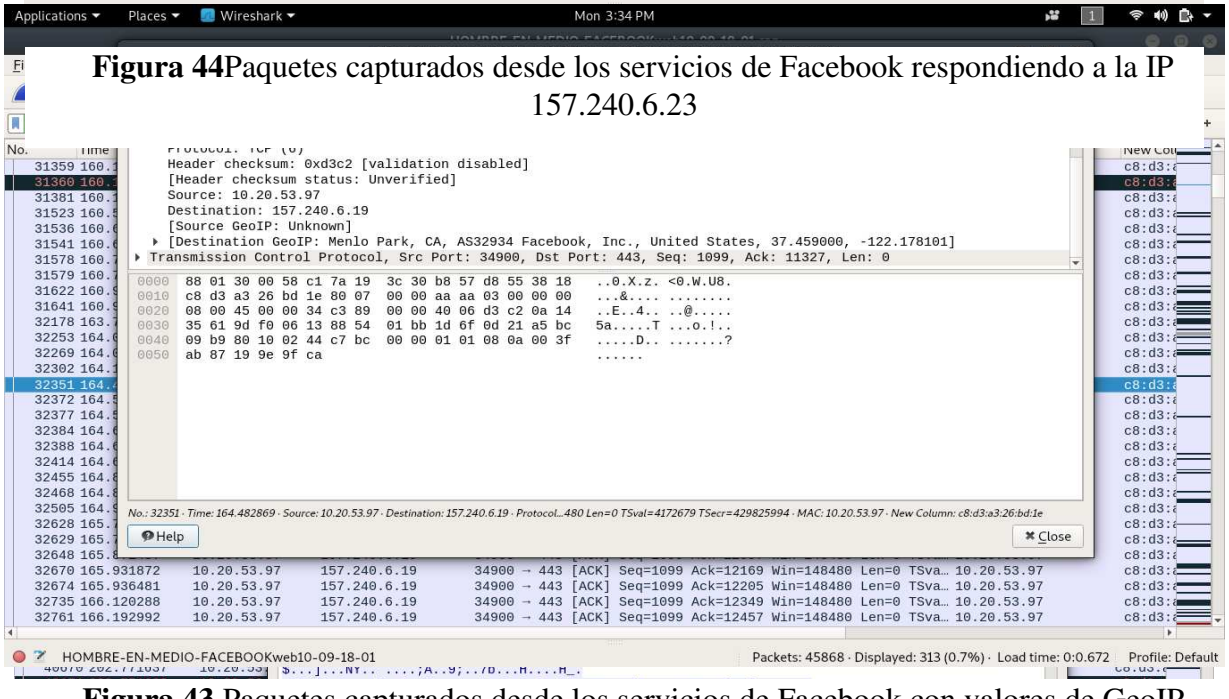

Figura 43 Paquetes capturados desde los servicios de Facebook con valores de GeoIP

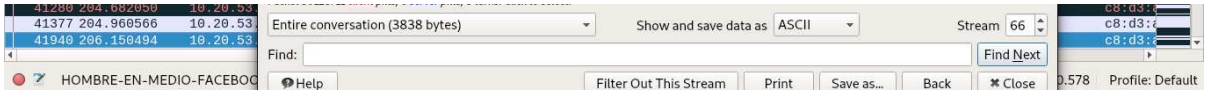

Figura 45 Paquetes capturados evidenciando su total encriptación

Se encuentra que pertenece a Facebook por los valores de geoip en el parámetro IPV4.

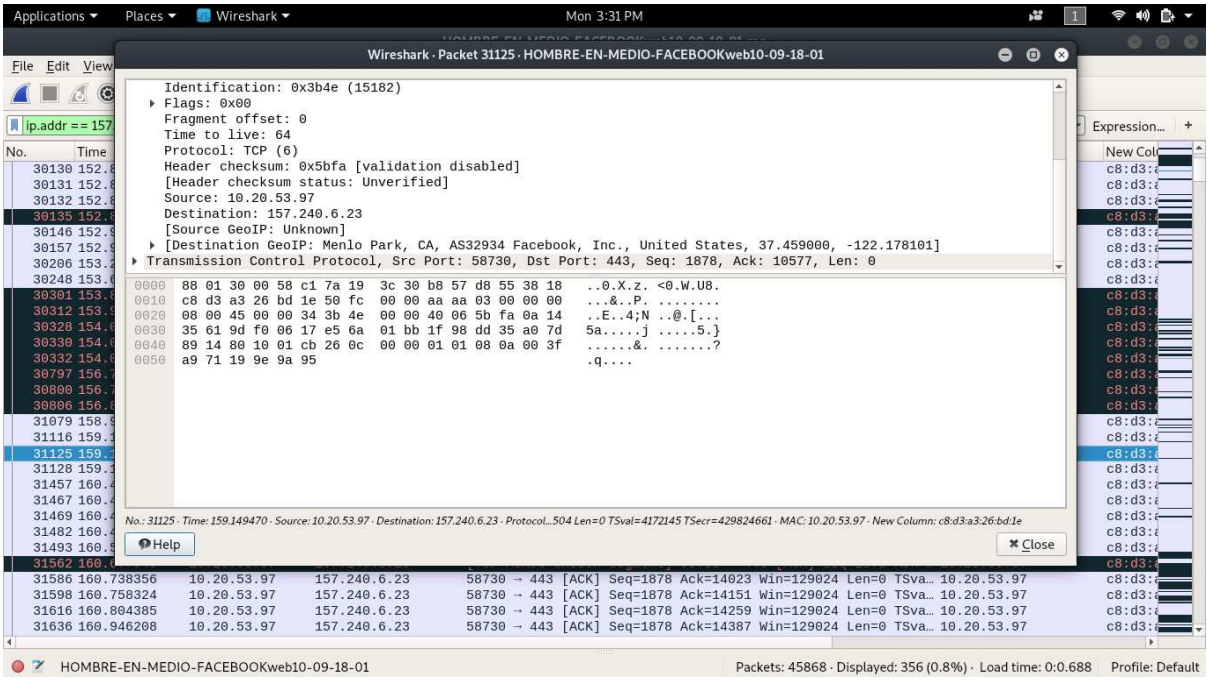

Figura 46 Paquetes capturados desde los servicios de Facebook con valores de GeoIP

Se identifican 2 servicios que teóricamente no deben involucrarse con Facebook. Se identificaron por la gran cantidad de tráfico generado logrando ubicar las direcciones IP´s.

Dos direcciones IP´s pertenecen a la empresa EPM Telecomunicaciones, la cual generó un total de 2.426 paquetes cifrados durante los 3 minutos de captura de datos únicamente frente a la aplicación de Facebook.

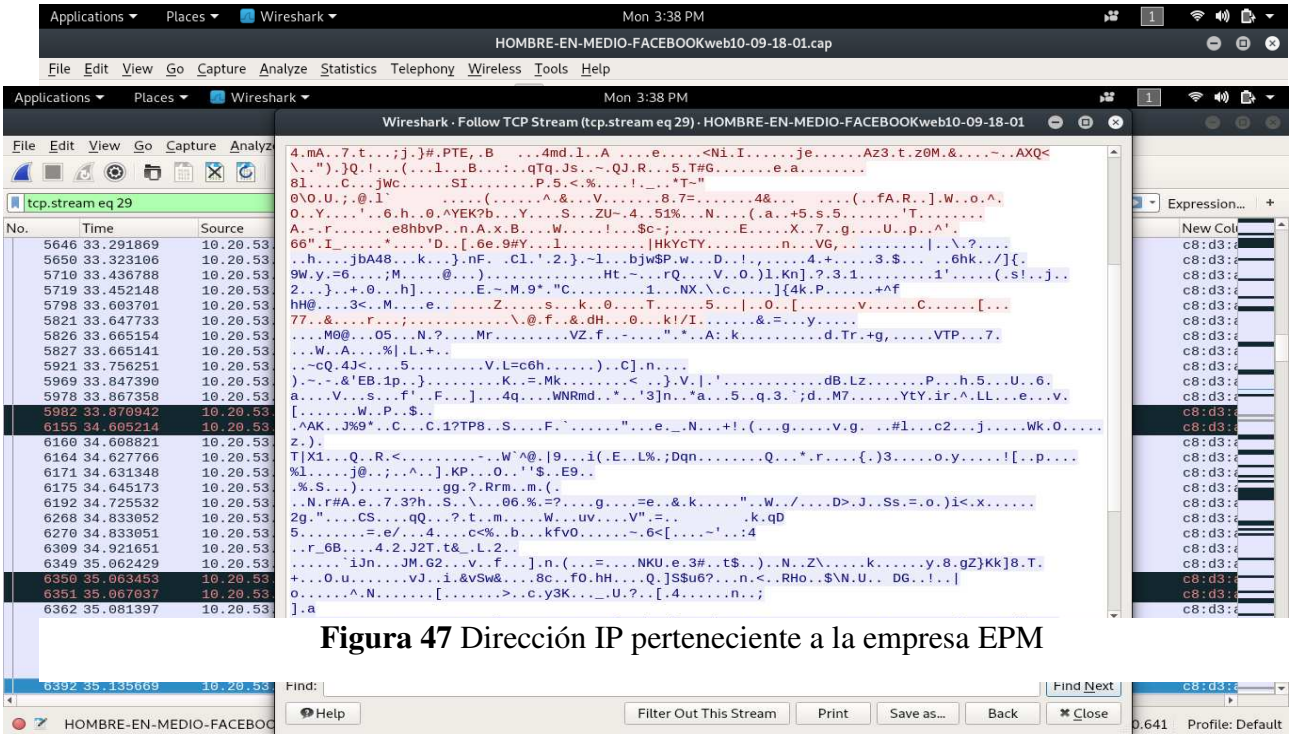

Figura 47 Dirección IP perteneciente a la empresa EPM

Figura 48 Trafico capturado de la IP de la empresa de EPM

Realizando una búsqueda superficial en la red acerca de convenios, alianzas o colaboraciones entre Facebook y EPM no se encontraron resultados relevantes para explicar el por qué el servidor con la dirección ip 200.114.57.81 ubicado en la ciudad de Medellín, Colombia está generando tráfico por medio de la aplicación de Facebook.

Se identifica que dicho servidor pertenece a EPM por las coordenadas y dominio asociado hallados en los valores de IPV4.

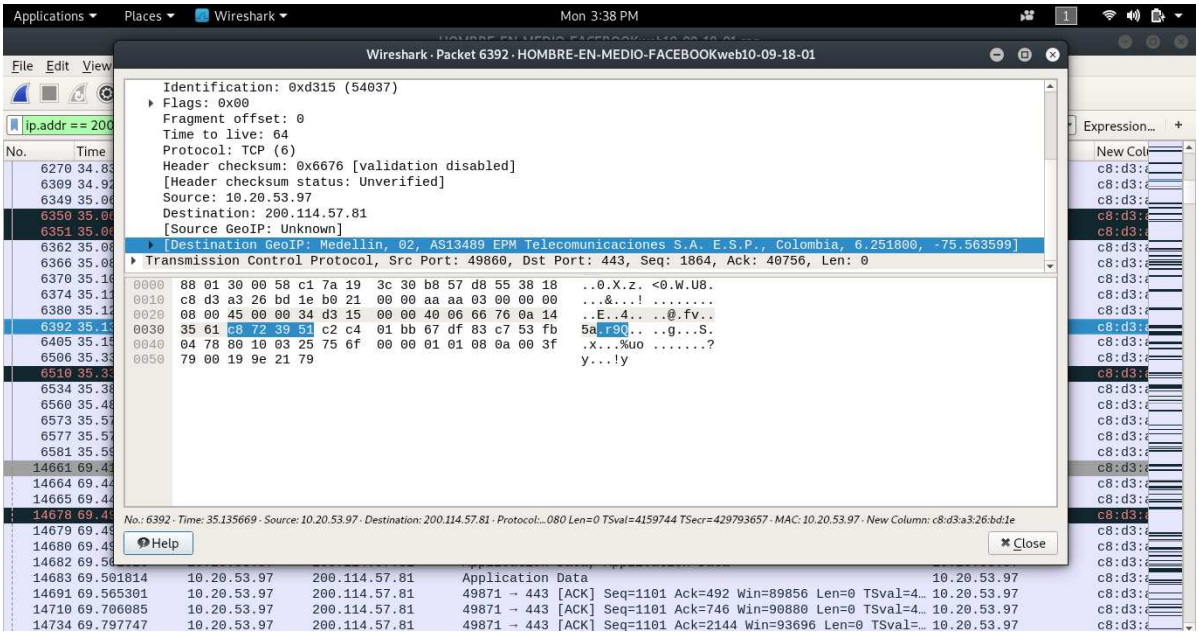

Figura 49 Paquetes capturados de la empresa EPM con su geolocalización

Otra dirección ip que generó bastante tráfico significativo es la 186.31.253.81. Esta dirección IP generó un total de 3397 paquetes cifrados, de los cuales se pudo obtener un pequeño dato que es significativo para analizar.

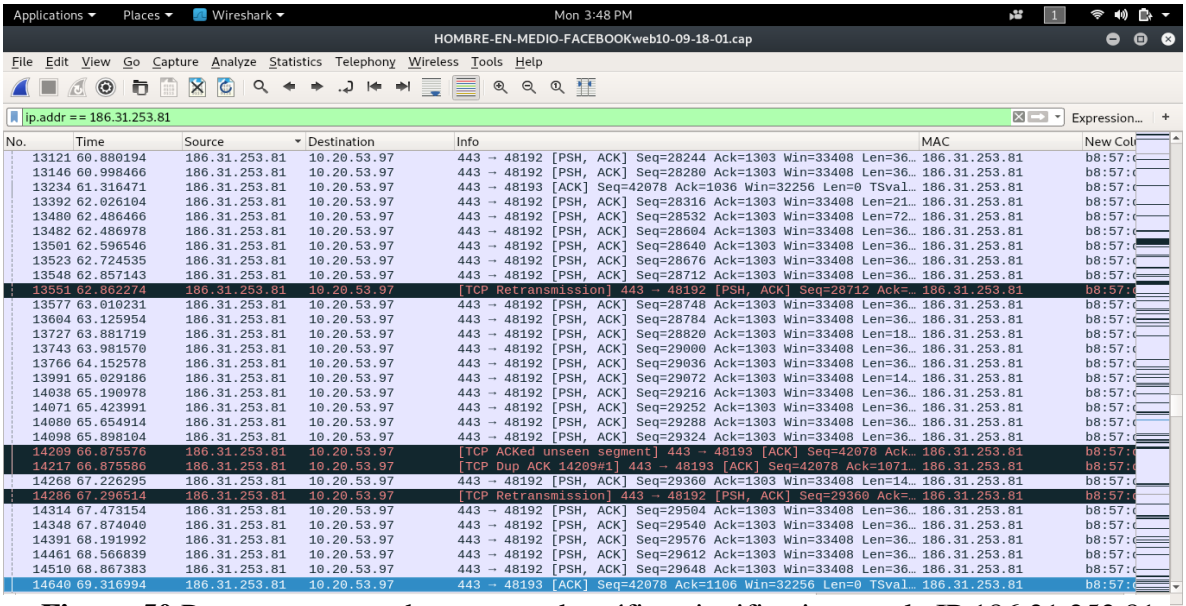

Figura 50 Paquetes capturados generando tráfico significativo con la IP 186.31.253.81

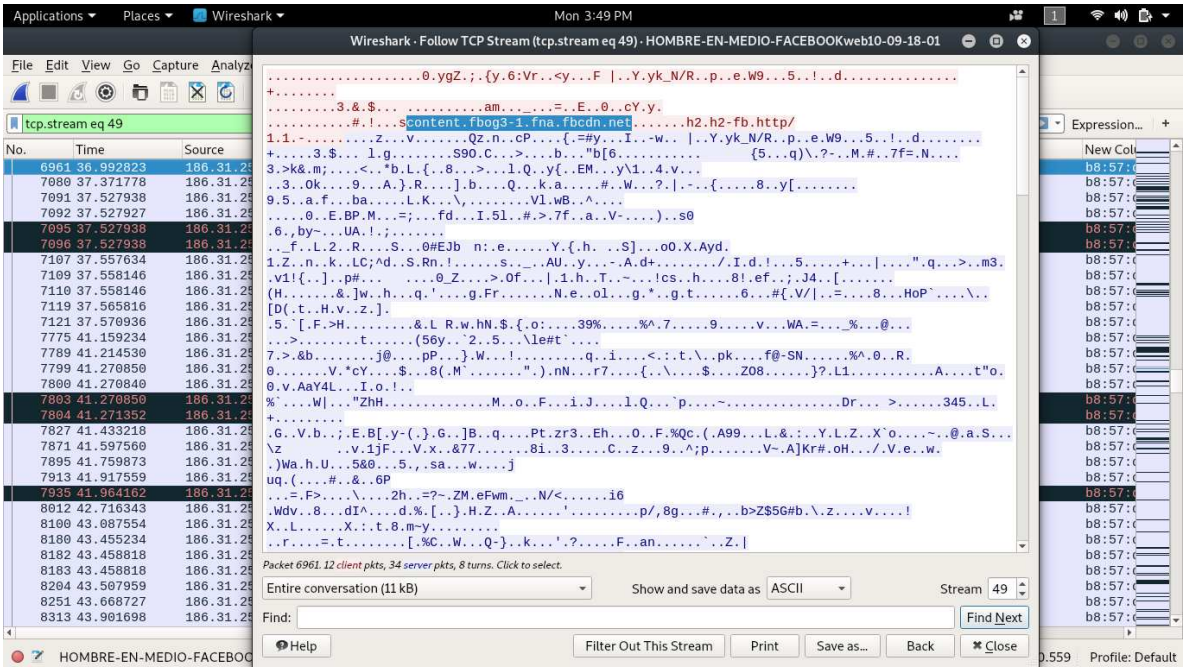

Figura 51 Paquetes capturados encriptados con encabezados de Facebook

En la captura de datos desde la dirección ip mencionada anteriormente, en uno de los paquetes analizado se encontró el siguiente contenido **scontent.fbog3-1.fna.fbcdn.net,** donde podemos revisar la captura de datos realizada a la ip **157.240.6.23** que responde directamente de un dominio de Facebook, se encuentra el siguiente contenido **xx.video.fbcdn.net** dentro de un paquete. Lo cual asegura que la dirección ip **186.31.253.81** que no tiene asociado ningún dominio en los valores GeoIP dentro de los parámetros de IPV4 y responde a coordenadas de la ciudad de Bogotá, Colombia, está generando u obteniendo tráfico a través de la aplicación de Facebook.

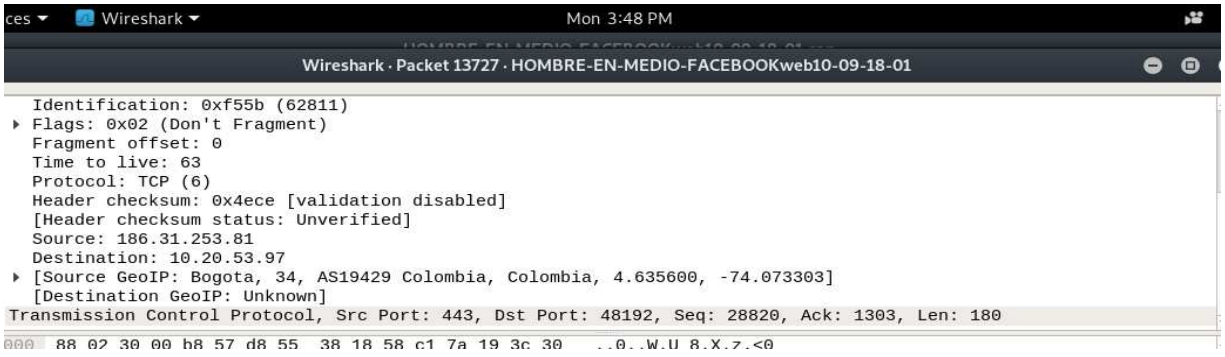

Figura 52 Paquetes capturados con geolocalización en Bogotá

Efectivamente Facebook cifra la información y protege la ubicación física de los servidores, pero se encuentran 2 inconsistencias de seguridad ya que no existen comunicados oficiales de por qué EPM está generando tráfico por medio de la aplicación de Facebook y por qué una dirección ip que no está asociada a un nombre reconocido, genera gran cantidad de tráfico desde el aplicativo de Facebook.

8.6 Prueba hombre en medio Siga UniAgustiniana

Dada la importancia de la plataforma de calificaciones de la universitaria agustiniana y el continuo uso que los estudiantes y docentes dentro de las instalaciones de la institución, se realiza una prueba sobre el aplicativo para conocer qué tan seguro es usar esta aplicación en una red WiFi abierta.

A través de un ataque de hombre en el medio, se realizó una captura de paquetes durante 3 minutos en los cuales se encontró la dirección IP privada del servicio, indicando que este servicio se aloja localmente en la red de la universitaria.

Se capturo un total de 19128 paquetes de los cuales el 100% está cifrado y sin posibilidades de ser interpretado.

Tabla 12

Numero de paquetes relevantes para las pruebas de la plataforma SIGA

IP	Servicio	Número de Paquetes	Porcentaje representativo en los datos capturados
172.16.1.10	SIGA	2705	14.1%

Sobre este servicio transita información bastante importante y relevante para cada usuario activo de la misma. Se encontró que el tráfico se encuentra cifrado protegiendo la integridad de la seguridad del usuario.

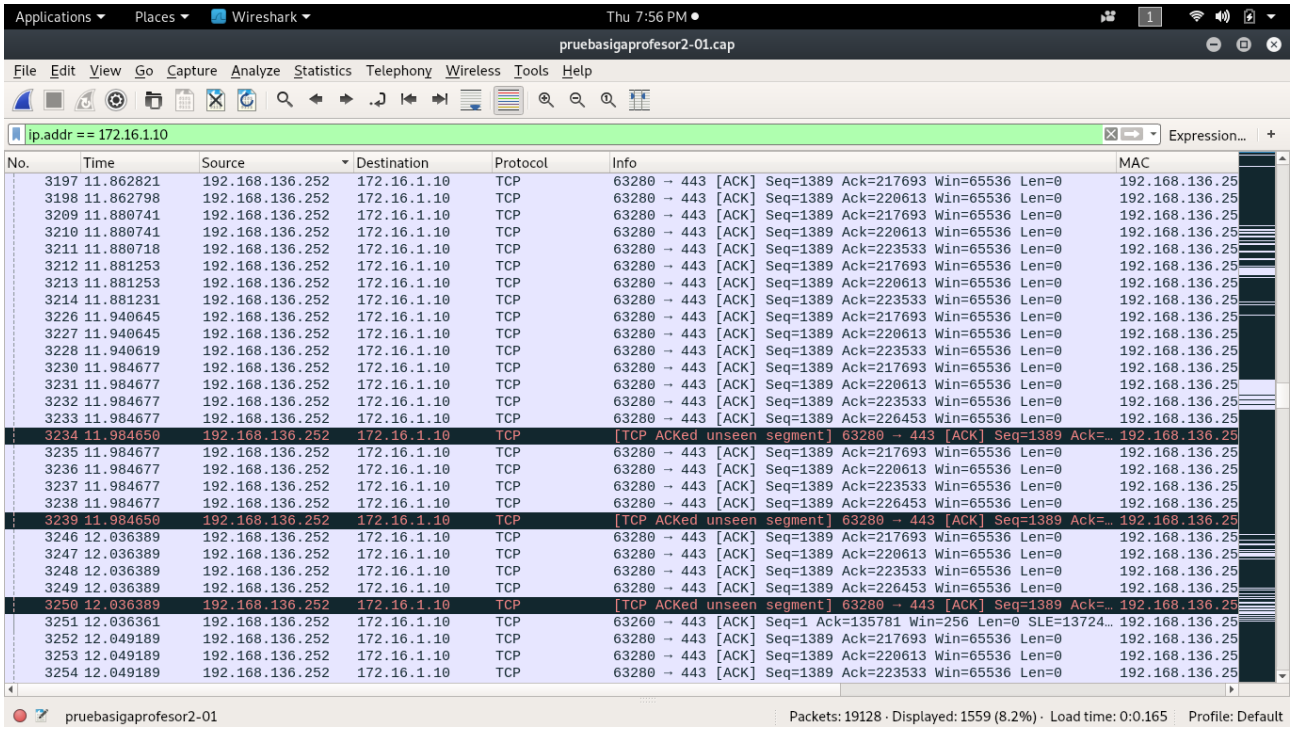

Figura 54 Trafico capturado del servicio del siga

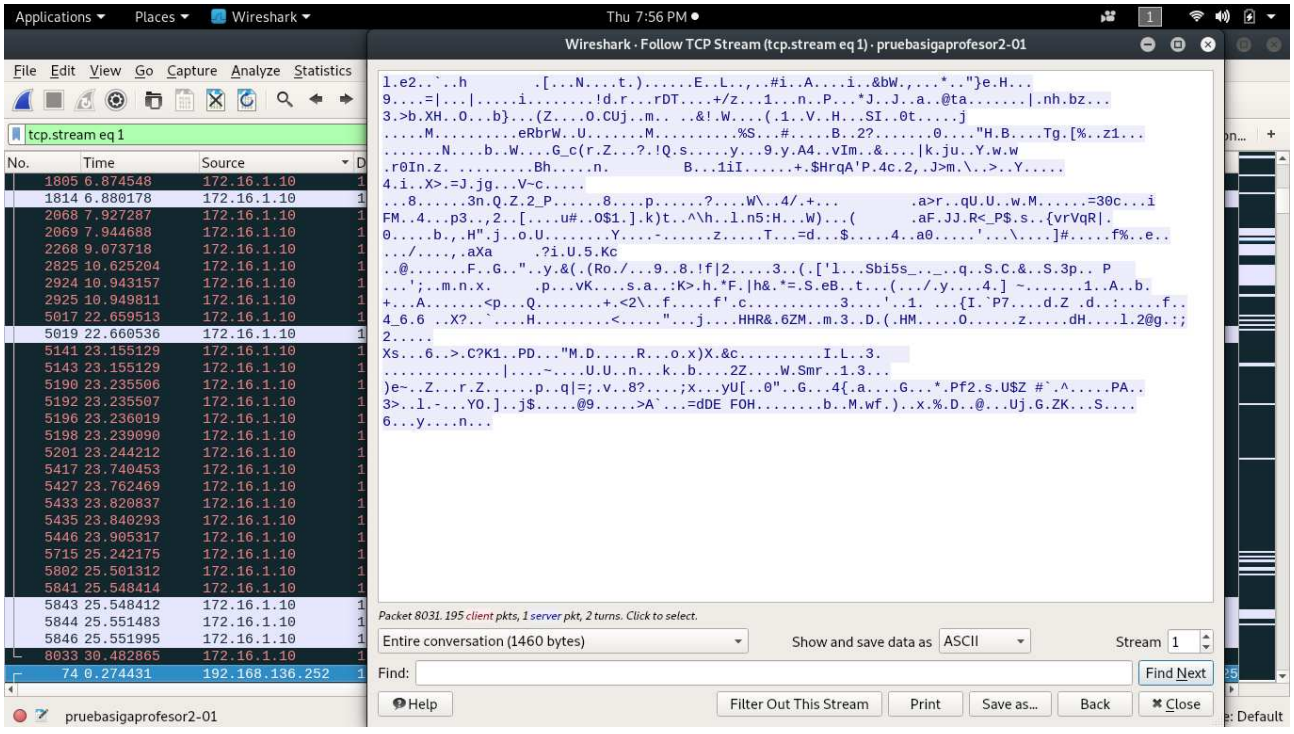

Figura 53 Trafico capturado del siga totalmente cifrado

Se comprobó que el servicio es seguro para sus usuarios, donde se asegura que una de las plataformas de mayor importancia en cuestión de la seguridad, cumple con los estándares mínimos de protección de la información.

9. Conclusiones

Se encontró que las redes wifi-abiertas en general proporcionan una gran brecha de seguridad y confidencialidad de los datos que generan los usuarios que usan este tipo de tecnologías, y por su falta de conocimiento, no se aseguran de tener buenas practicas al momento de navegar en este tipo de redes.

Se concluyó que hay bastantes puntos débiles o vulnerabilidades que afectan a las redes wifi-abiertas siendo la ingeniería social, el cache, el medio de transmisión y los tres principales pilares que fundamentan la mayoría de los ataques a este tipo de tecnología.

Se logró explotar los puntos más débiles de las redes wifi-abiertas, encontrando información sensible para los usuarios en 2 de los 3 aplicativos estudiantiles de la universitaria agustiniana, realizando un diagnóstico de seguridad malo para la reputación de estos.

Se encontraron métodos para los usuarios finales que aseguran principalmente los ataques basados en las vulnerabilidades encontradas, que se pueden aplicar a cualquier tipo de red wifi abierta.

10. Recomendaciones

Luego de realizar el análisis descrito anteriormente, se recomienda revisar cuando se realicen navegaciones, que sean páginas con uso de protocolo https para evitar que el tráfico sea capturado e interpretado de manera completamente segura.

Se recomienda no realizar transacciones o ingresar información sensible cuando se esté navegando en una red wifi abierta y utilizar en lo posible este tipo de redes únicamente para usos recreativos.

Si es necesario realizar algún movimiento o algún tipo de navegación que genere algún impacto en la privacidad o seguridad de los datos del usuario, se puede hacer uso de aplicativos que generen una conexión VPN de manera gratuita.

Para comprobar este método, se realizó una pequeña captura de datos sobre el portal de aulas virtuales de la Universitaria Agustiniana, el cual en pruebas anteriores se comprobó que la información de acceso de un usuario es totalmente vulnerable. Se comprobó que por medio de un aplicativo que genera gratuitamente una VPN a algún país seleccionado, todo el tráfico es cifrado para evitar ataques de hombre en el medio.

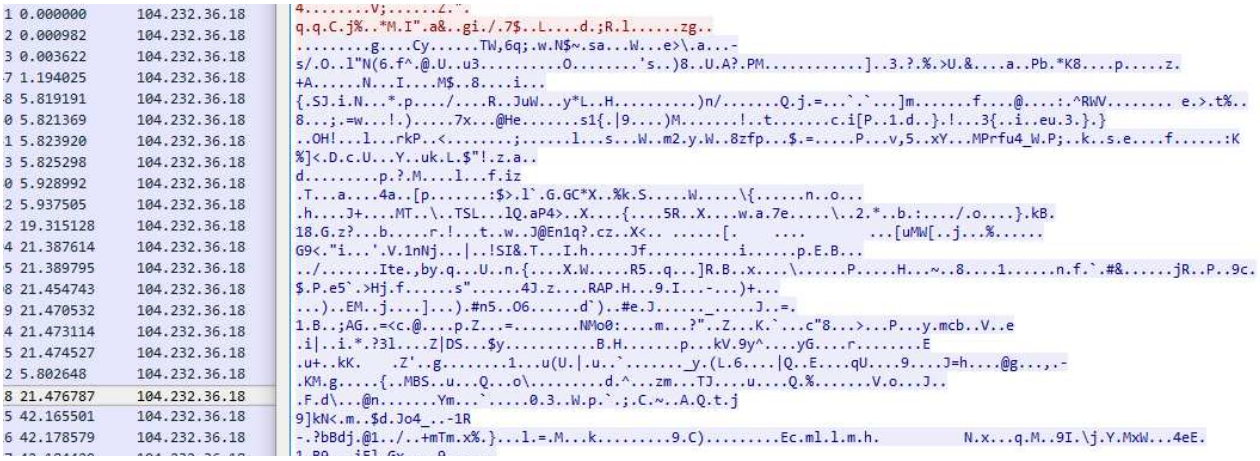

Figura 55 Trafico encriptado de la VPN

El aplicativo cambia la dirección IP que responde la solicitud, haciendo que el tráfico sea encriptado y al momento de ser capturado no sea interpretado. Cabe resaltar que la información que llega al servidor con el cual se enlaza la VPN tendrá acceso al tráfico completamente vulnerable tal y como si se hubiera generado sin dicha conexión.

Se puede usar aplicativos VPN de pago o privados para aumentar la seguridad y las pólizas que dicho servicio le preste al usuario.

11. Bibliografía

acens. (2012). *Acens, The cloud services company.* Obtenido de https://www.acens.com/wp-content/images/whitepaper-redes-seguridad-acens-julio-2012.pdf

Ching-Chuan Wei, Chi-Han Yu, & Lawrence Chiang. (s.f.). *IEEE Xplore*. Obtenido de IEEE Xplore: http://ieeexplore.ieee.org/document/8008629/

chiu, s. h. (s.f.). *Seguridad en Redes Inalámbricas 802.11.*

Ciens. (s.f.). *Ciens*. Obtenido de Ciens: http://www.ciens.ucv.ve:8080/genasig/sites/redesmov/archivos/Seguridad%20en%20Redes%20Inalambricas%20802.pdf

IEEE. (2016). *IEEE*. Obtenido de http://standards.ieee.org/findstds/standard/802.11-2016.html

Ieee Explore. (30 de 03 de 2017). Obtenido de http://sci-hub.cc/http://ieeexplore.ieee.org/document/7889332/

Maps, G. (s.f.). *Google Maps*. Obtenido de Google Maps: https://maps.google.com/

MinTic. (1989). *Ministerio de telecomunicaciones* . Obtenido de Ministerio de Telecomunicaciones : http://www.mintic.gov.co/portal/604/w3-channel.html

MinTic. (1990). *Ministerio de telecomunicaciones* . Obtenido de Ministerio de telecomunicaciones .

MinTic. (18 de 08 de 1990). *MinTic*. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3568.html

MinTic. (2009). *Ministerio de telecomunicaciones* . Obtenido de Ministerio de telecomunicaciones .

MinTic. (29 de Julio de 2009). *MinTic*. Obtenido de MinTic: http://www.mintic.gov.co/portal/604/w3-article-3707.html

MinTic. (29 de 07 de 2009). *MinTic*. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3707.html

MinTic. (13 de 10 de 2009). *MinTic*. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3770.html

MinTic. (2012). *Ministerio de telecomunicaciones*. Obtenido de Ministerio de telecomunicaciones .

MinTic. (10 de 03 de 2013). *MinTic*. Obtenido de MinTic: http://www.mintic.gov.co/portal/604/w3-article-3799.html

MinTic. (30 de 01 de 2013). *MinTic*. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3823.html

MinTic. (28 de 04 de 2013). *MinTic*. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3371.html

MinTic. (19 de 12 de 2016). *MinTic*. Obtenido de http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html

MinTic. (03 de 10 de 2017). *MinTic*. Obtenido de MinTic: http://www.mintic.gov.co/portal/604/w3-article-61000.html

Websec. (2013). *Websec*. Obtenido de Websec: http://www.websec.mx/publicacion/blog/estadisticas-redes-wifi-80211-mexico-2013

12. Lista de figuras

13. Lista de tablas

14. Anexos

5 Paquetes capturados de la prueba realizada al aplicativo de WhatsApp - https://www.dropbox.com/s/c3iepk5o9etuu5p/CLI_Book_5.5R5-1.pdf?dl=0

6 Paquetes capturados de la prueba realizada al aplicativo de Facebook - https://www.dropbox.com/s/c3iepk5o9etuu5p/CLI_Book_5.5R5-1.pdf?dl=0

7 Paquetes capturados de la prueba realizada al aplicativo de Gmail APP - https://www.dropbox.com/s/c3iepk5o9etuu5p/CLI_Book_5.5R5-1.pdf?dl=0

8 Paquetes capturados de la prueba realizada al aplicativo de Gmail Web - https://www.dropbox.com/s/c3iepk5o9etuu5p/CLI_Book_5.5R5-1.pdf?dl=0

9 Paquetes capturados de la prueba realizada al aplicativo de Siga Uniagustiniana - https://www.dropbox.com/s/c3iepk5o9etuu5p/CLI_Book_5.5R5-1.pdf?dl=0

10 Paquetes capturados de la prueba realizada al aplicativo de Aulas Virtuales Uniagustiniana - https://www.dropbox.com/s/c3iepk5o9etuu5p/CLI_Book_5.5R5-1.pdf?dl=0

11 Paquetes capturados de la prueba realizada al aplicativo de Biblioteca virtual Uniagustiniana- https://www.dropbox.com/s/c3iepk5o9etuu5p/CLI_Book_5.5R5-1.pdf?dl=0