Hacking in WEB services through open WIFI networks

Hacking en servicios WEB a través de redes WIFI abiertas

Francisco Clemente Valle Díaz[1] Carlos Steveen Herrera Gonzáles[2], Cristian Steven Pedraza Castro[3]
[1]*francisco.valle@uniagustiniana.edu.co*, [2]*carlos.1996.h@hotmail.com*, [3]*stivenpedraza_12@hotmail.com*

Universitaria Agustiniana. Bogotá, Colombia
Artículo de Investigación

Resumen

El uso en los diferentes sectores de las redes de acceso a internet a través de tecnología WIFI se ha vuelto bastante común en nuestros días, en entornos educativos se observa frecuentemente como los estudiantes realizan uso constante de redes abiertas, para obtener acceso a populares redes sociales, así como a los diferentes servicios que ofrecen las instituciones educativas en internet, sin tener conciencia de los riesgos en materia de ciber seguridad a los que se exponen. En el presente trabajo se realiza un ataque a la información que circula en redes WIFI abiertas, enfocados en el tráfico de información que se genera durante una conexión entre el punto de acceso inalámbrico y un usuario. Se realizaron diferentes pruebas dentro de la Universitaria Agustiniana, donde mediante el uso diferentes equipos y componentes de telecomunicaciones se simuló el tráfico generado al consultar diferentes servicios web.

Se implementó un ataque tipo HOMBRE EN EL MEDIO poniendo a prueba diferentes servicios utilizados por los estudiantes dentro de la Universitaria Agustiniana tales como WhatsApp, Facebook, correo electrónico y aplicativos de uso institucional como las aulas virtuales y el aplicativo web de la biblioteca.

Después de realizado el ataque y con los datos capturados se efectúa un análisis de la data capturada mediante la herramienta WIRESHARK dentro del sistema operativo KALI LINUX, en donde se observa que la navegación en algunas de las aplicaciones no cifra los datos, esta vulnerabilidad puede ser explotada con éxito para obtener datos sensibles de los usuarios de dichas redes. También se evidencia que aplicaciones que implementan una VPN, pueden convertirse en una herramienta de seguridad efectiva al momento de consultar servicios que no utilizan cifrado mientras se navega mediante redes WIFI abiertas.

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

1. INTRODUCCIÓN

En nuestros días los avances tecnológicos nos permiten vivir conectados a internet desde diversos lugares, las redes de acceso inalámbrico a internet que operan bajo el estándar de comunicaciones 802.11 (WIFI) se han vuelto populares para este fin y su presencia es común en diferentes entonos como los educativos [1], y los centros comerciales. En estos últimos observó que en un promedio de 11 minutos se conectan alrededor de 6407 dispositivos a estas redes [2], dicha popularidad sumada al esfuerzo que realizan los diferentes gobiernos por garantizar el acceso a internet a sus ciudadanos, han permitido el despliegue y uso de numerosas redes WIFI de acceso gratuito a internet, sin embargo los esfuerzos enfocados en concientización en temas de seguridad informática no crecen al mismo nivel. [3], [4].

Se estima que en el 2017 los costos anuales asociados a violaciones de datos para la empresa alcanzaron en promedio unos US $ 3.86 millones, según datos presentados por el anual “data breach report” patrocinado por IBM [5] y que durante el 2018 los grupos de ataque dirigidos continuaron representando una amenaza significativa para las organizaciones, los 20 grupos más activos seguidos por Symantec lograron un promedio de 55 organizaciones en los últimos tres años, frente a los 42 entre 2015 y 2017.[6]

El éxito de un gran número de ataques se debe en parte a la falta de conocimiento de ciberseguridad por parte de los individuos [7]. Esto a pesar de los esfuerzos realizados por los investigadores de seguridad

informática a través de los cuales se pretende prevenir e identificar las numerosas formas de ataques que pueden sufrir las redes WIFI.[8]-[19].

2. MÉTODO

2.1 Hacking de datos en redes abiertas.

En el desarrollo de la presente investigación, se realizara un ataque conocido como hombre en el medio [20]–[23] (traducido del inglés MITM) en una red WIFI abierta. En virtud de que el medio de comunicación mediante el cual se trasmiten los datos en una red WIFI es el espacio, es posible capturar los datos trasmitidos tanto por el access point como por cualquier dispositivo que se encuentre conectado a este, simplemente ubicándose dentro de su rango que cobertura y configurando una tarjeta de red en modo monitor, de manera que esta capture los paquetes que sean dirigidos a cualquier dispositivo de red.
En el desarrollo de la presente investigación se utilizaron los siguientes elementos técnicos (hardware y software), en el proceso de hacking:

1. AP E410 Cambium.
2. Computador portátil Dell latitude – Como dispositivo atacante
3. Computador portátil Asus X540Y – como dispositivo víctima.
4. Sistema operativo Kali Linux, el cual es un proyecto de código abierto mantenido y financiado por Offensive Security.
5. Wireshark – Un analizador del protocolo de red.
6. Suite de Aircrack-NG

Para realizar el ataque conocido como "hombre en el medio" se configura una red inalámbrica abierta con el SSID de "VIRUS-NO-CONECTAR" de manera que este nombre desincentive la conexión a dicha red de las personas que se encontraran dentro de su área de cobertura y no forman parte del equipo investigador (esto con el fin de no vulnerar sus datos).

En el computador que fungirá como máquina atacante se utiliza la suite Aircrack-ng con el fin obtener toda la información que se envía entre el access point y el computador de la víctima, desde el cual se consultaran los diferentes servicios web. Para logar la captura de paquetes en la máquina atacante se siguen los siguientes pasos:

1. Configurar en el dispositivo atacante la tarjeta inalámbrica de red en modo monitor, escribiendo en una terminal el comando "airmon-ng start wlan0", con lo cual se habilita la interface inalámbrica (wlan0) en modo monitor para la captura de paquetes.

2. Se identifica el access point – AP, sobre el cual se realizará el ataque, su dirección MAC y el canal en el cual trasmiten los datos, mediante la instrucción "airodump-ng waln0mon".

    a. Dirección MAC - 58:C1:7A:19:3C:30
    b. Canal 6

3. Se configura la máquina atacante para capturar el tráfico entrante y saliente del AP donde se encuentra conectado el equipo víctima, mediante el comando "airodump-ng -c 6 --bssid 58:c1:7a:19:3c:30 -w HOMBRE-EN-MEDIO wlan0mon", los datos obtenidos se guardan con el nombre de HOMBRE EN MEDIO para su posterior análisis.

La totalidad del trafico capturado se analiza con Wireshark.

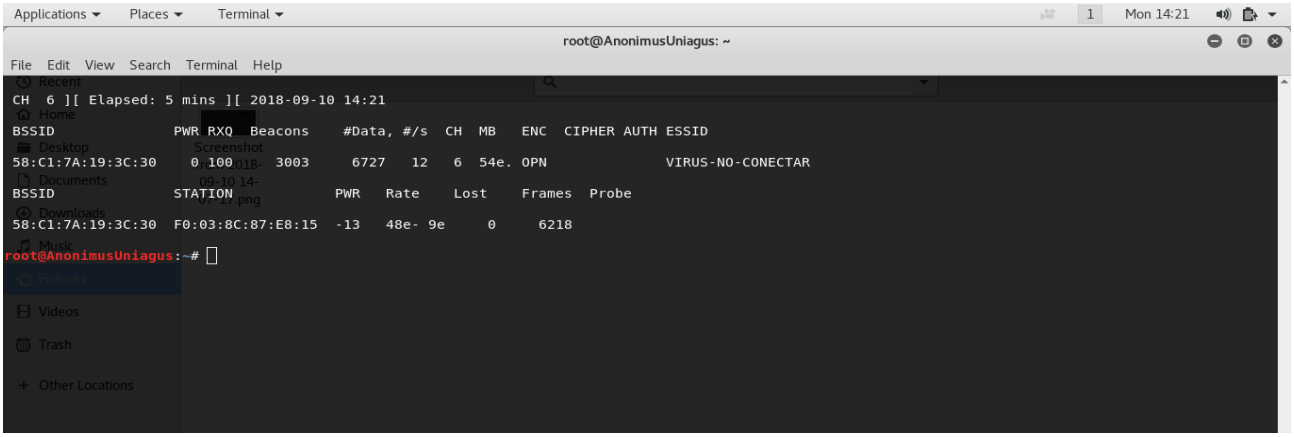


Figura 1. – Pantallazo de la captura de datos

2.2 Servicios sobre los cuales se realiza la captura del tráfico.

En todos los casos el computador asociado a la víctima se conectó a internet utilizando como pasarela la red abierta implementada con tecnología WIFI llamada "VIRUS-NO-CONECTAR", al tiempo que desde el equipo configurado como máquina atacante se realizaba la captura de los datos asociados con el access point.

Se realizó captura de tráfico respecto de la navegación en diferentes servicios, algunos asociados a entornos universitarios y otros relacionados con actividades sociales con el animo de simular entornos reales en nuestros días.

El primer servicio elegido para el análisis es la plataforma de aulas virtuales de la universitaria Uniagustiniana, esta plataforma es utilizada por estudiantes y docentes de la Uniagustiniana como apoyo en los procesos académicos llevados al interior de la institución.

El segundo servicio analizado fue la biblioteca virtual de la Uniagustiniana, de uso continuo para la consulta revisión y/o renovación del material disponible en la biblioteca.

El tercer servicio analizado es la popular plataforma de comunicaciones WhatsApp, la cual para tranquilidad de sus usuarios notifica que toda la información trasmitida a través de la misma se encuentra protegida con cifrado de extremo a extremo.

El cuarto servicio analizado es la red social Facebook comúnmente frecuentada por jóvenes y utilizada como medio de comunicación masivo.

El quinto servicio sobre el cual se realiza la captura de datos el de correo electrónico, de uso común en ambientes educativos y empresariales.

3. RESULTADOS

3.1 Captura – Aulas virtuales Uniagustiniana

El ataque se efectuó en un estimado de 3 minutos, tiempo durante el cual desde el computador de la víctima se generó uso de la plataforma por parte de uno de los investigadores. En total se capturaron 54950 paquetes, de los cuales 2649 son provenientes de la plataforma virtual de asignaturas, se observó que el 100% del tráfico se encuentra sin cifrado.

Tabla 1. Estadística de paquetes capturados

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

Al analizar los datos capturados con el PC atacante se obtuvo el usuario y la contraseña utilizados desde el equipo víctima (Usuario: 1920141021; Password: c4rlit05), contenido grafico de los cursos y datos de otros estudiantes asignados a una misma asignatura, así como información de un curso preparatorio para el examen saber pro.

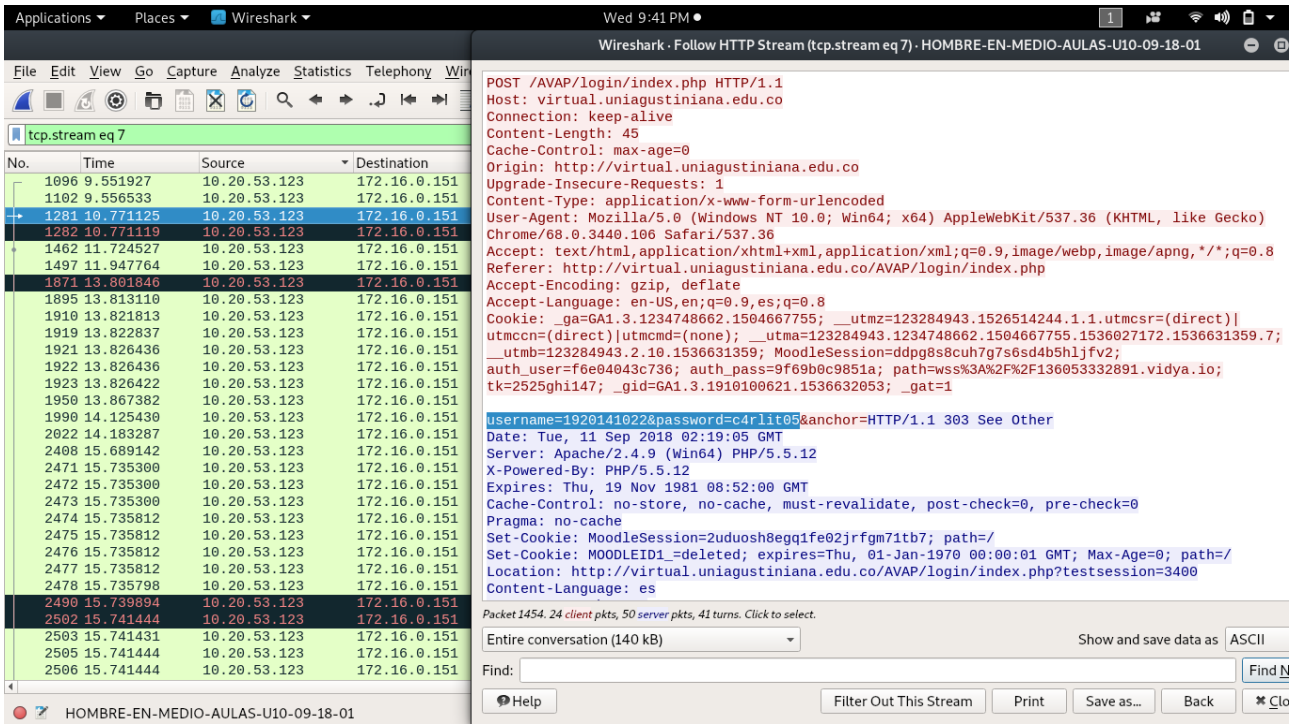


Figura 2. – Información capturada de Aulas virtuales

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

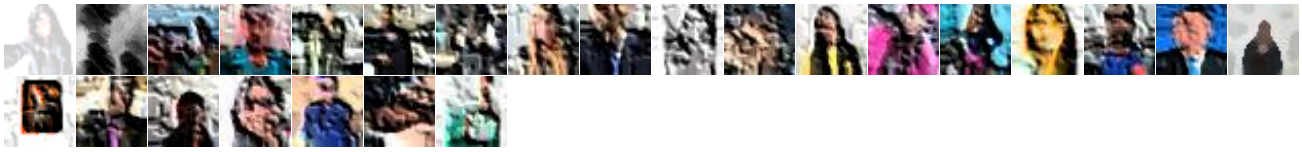


Figura 3. – imágenes obtenidas en la captura

3.2 Captura – Biblioteca virtual Uniagustiniana

El ataque se efectuó en un estimado de 3 minutos, al analizar el tráfico de datos capturados se identificó que el mismo se envía en texto plano, pudiendo capturar las credenciales de acceso del usuario víctima del ataque. (UserIS:1920141022 y su Password:1014278670)

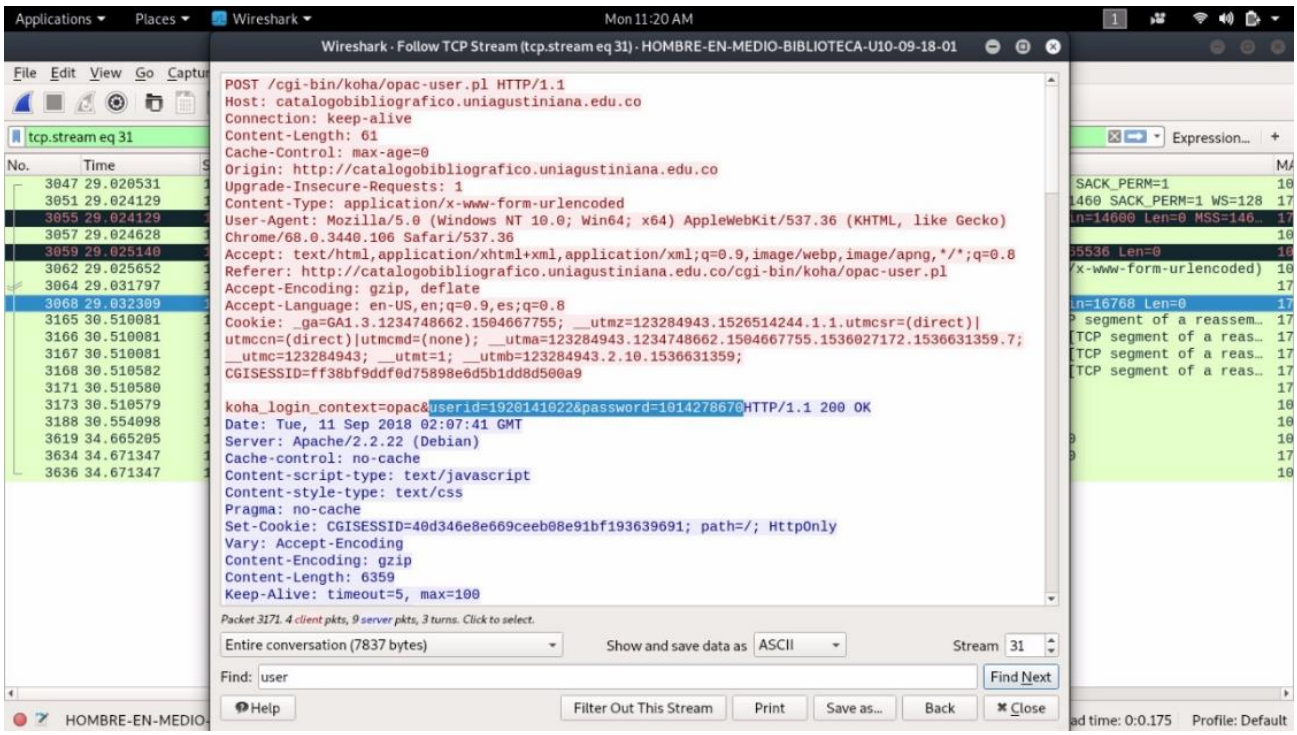


Figura 4. – Datos capturados en texto plano

3.3 Captura – WhatsApp Web

El ataque se efectuó en un estimado de 3 minutos, tiempo durante el cual desde el computador de la víctima se enviaron datos a través de la aplicación WhatsApp Web. Sobre el tráfico obtenido desde el computador del atacante, se identificó la dirección IP pública (157.240.14.53) que responde a las solicitudes enviadas por el cliente, así como las coordenadas geográficas asociadas a la misma “37°27'32.4"N 122°10'41.2"W” ubicadas en la ciudad de Menlo Park, California y asociado a Facebook Inc.

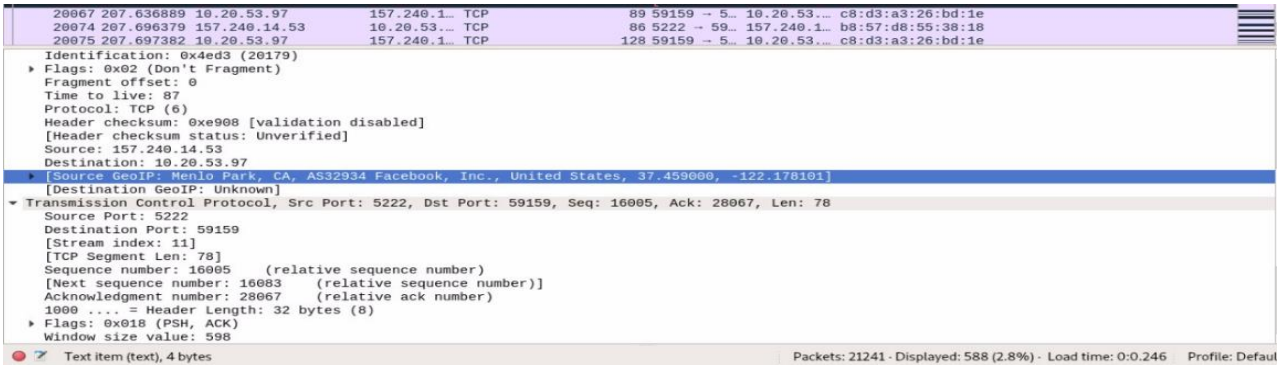


Figura 5.-Geolocalización de la IP capturada

Al verificar la información de georreferenciación de la dirección IP obtenida, se identifica que la misma pertenece a una zona residencial, por lo cual se estima que las peticiones son respondidas por un servidor fantasma.

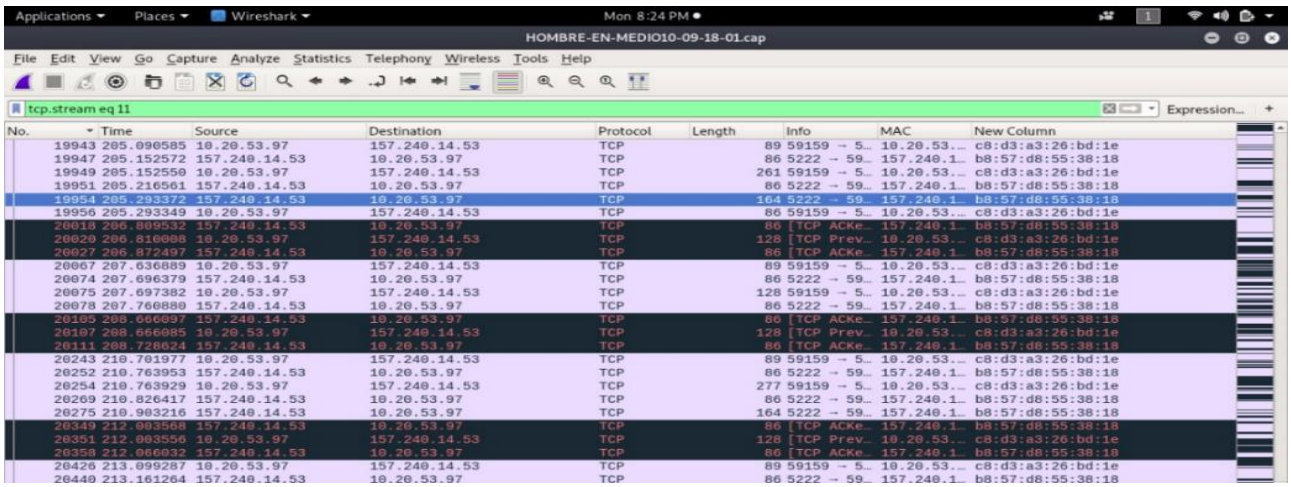


Figura 6.-Captura de tráfico WhatsApp Web

Al revisar el tráfico capturado, se identifica que toda la información asociada al proceso de comunicación se encuentra cifrada.



Figura 7.-datos cifrados trasmitidos por WhatsApp Web

3.4 Captura - Facebook

En ataque se realizó durante un tiempo estimado de 3 minutos, en la captura de datos realizada respecto de la red social Facebook se generó tráfico desde el computador de la víctima, simulando el uso normal que se realizaría de dicha red. Capturando un total de 45.868 paquetes, de los cuales se identificó que 6834 contenían tráfico asociado a la red social

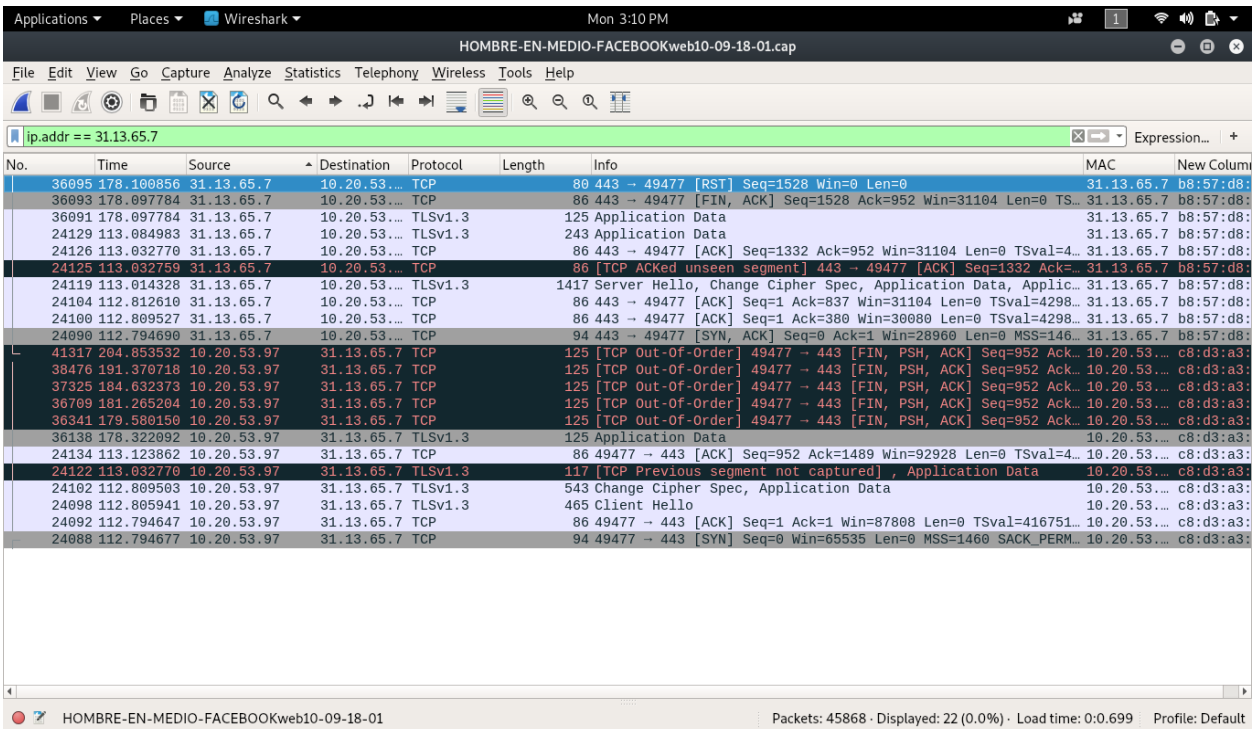


Figura 8.-Captura de datos - Facebook

En la tabla No 2 se presenta la información de las direcciones IP públicas utilizadas en el proceso de comunicación.

Tabla 2. Estadística de paquetes capturados - 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 cinco direcciones IP asociadas a la compañía Facebook (ubicadas en Menlo Park y en Dublín, Irlanda) manejan un sistema de seguridad similar al identificado en la aplicación WhatsApp, es decir estos utilizan servidores fantasmas que responden y reenvíen las solicitudes. De igual manera se observa que todo el tráfico relacionado con las mismas se encuentra cifrado.

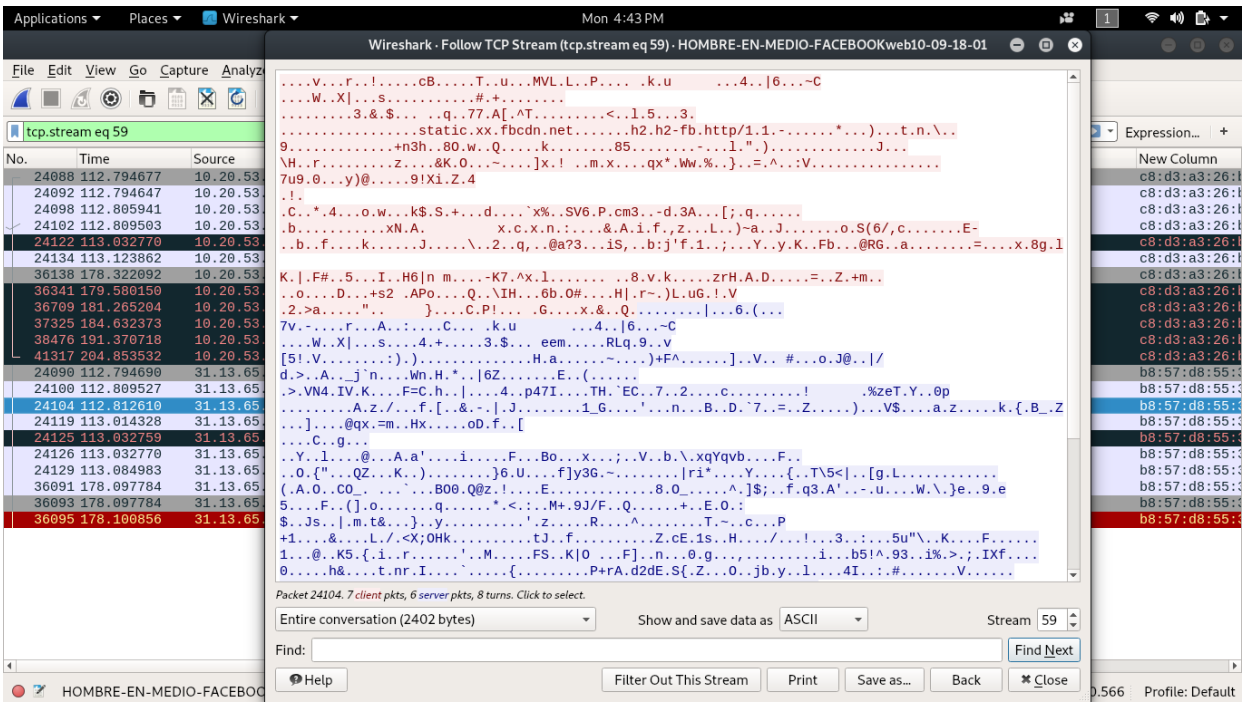


Figura 9.-comunicación cifrada relacionada con la IP 31.13.65.7

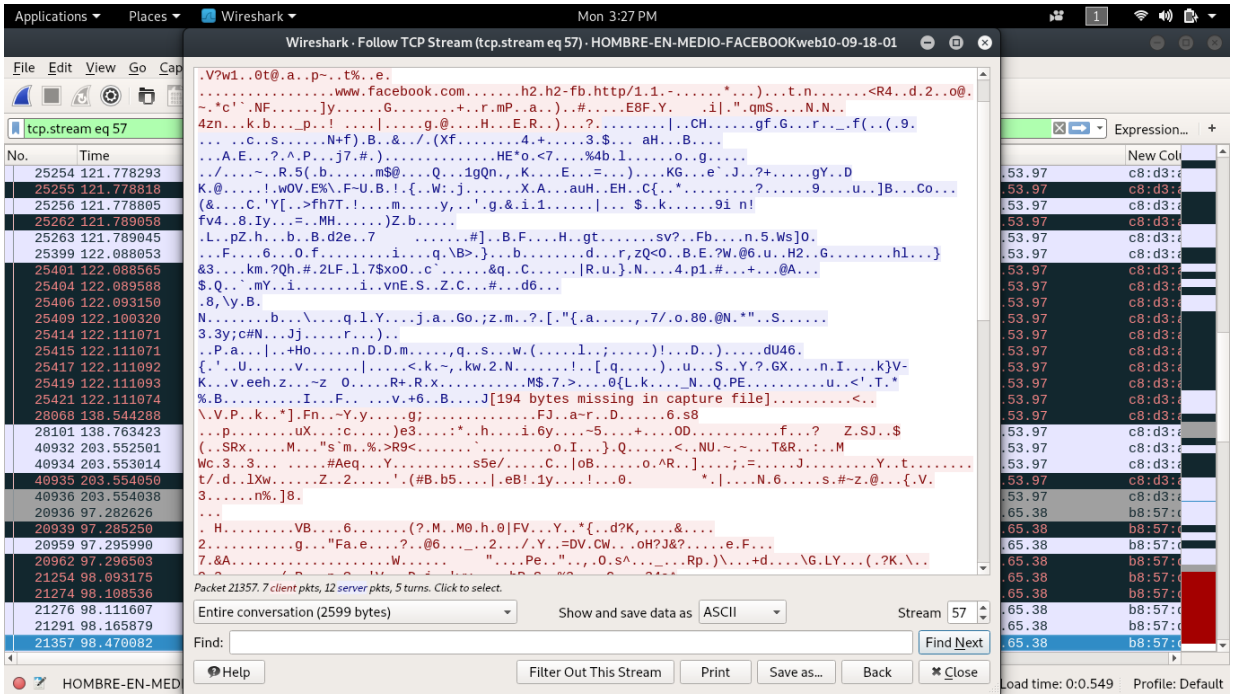


Figura 10.- comunicación cifrada relacionada con la IP 31.13.65.38

Se identifica que dos direcciones IP ubicadas en la ciudad de Medellín pertenecientes a la empresa EPM Telecomunicaciones, que gestionan parte del tráfico generado al consultar la red social.

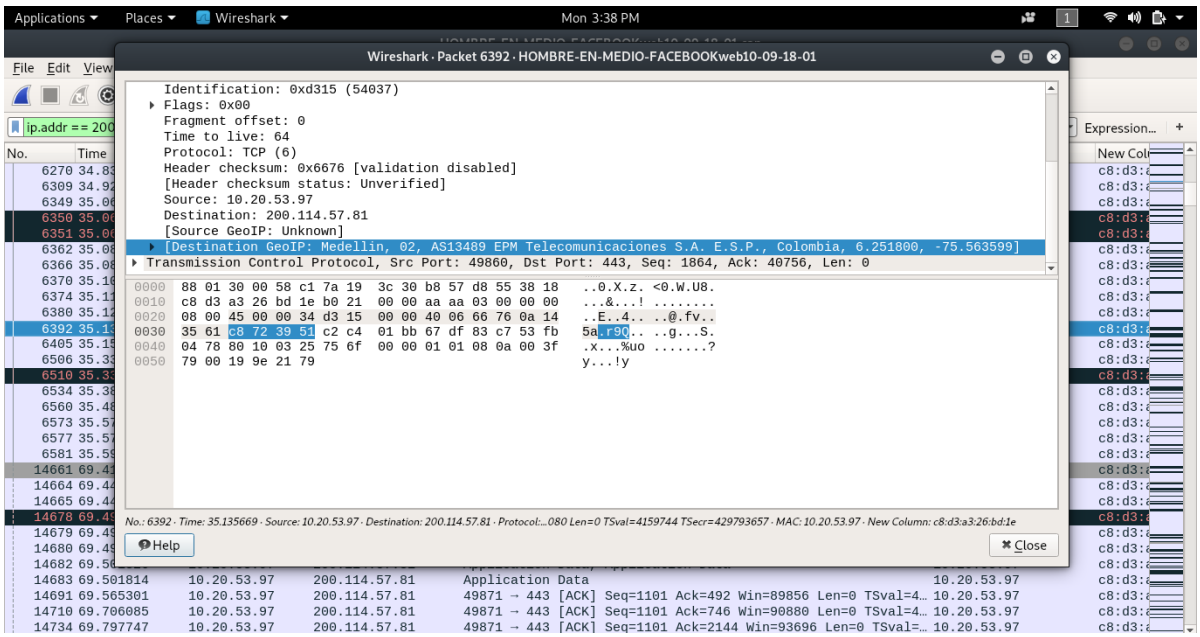


Figura 11.- comunicación relacionada con la IP 200.114.57.81

El tráfico generado por los servidores ubicados en la ciudad de Medellín también se encuentra cifrado.



Figura 12.- tráfico cifrado de servidor en Medellín

En la captura también se identifica en uno de los paquetes analizados la información “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.

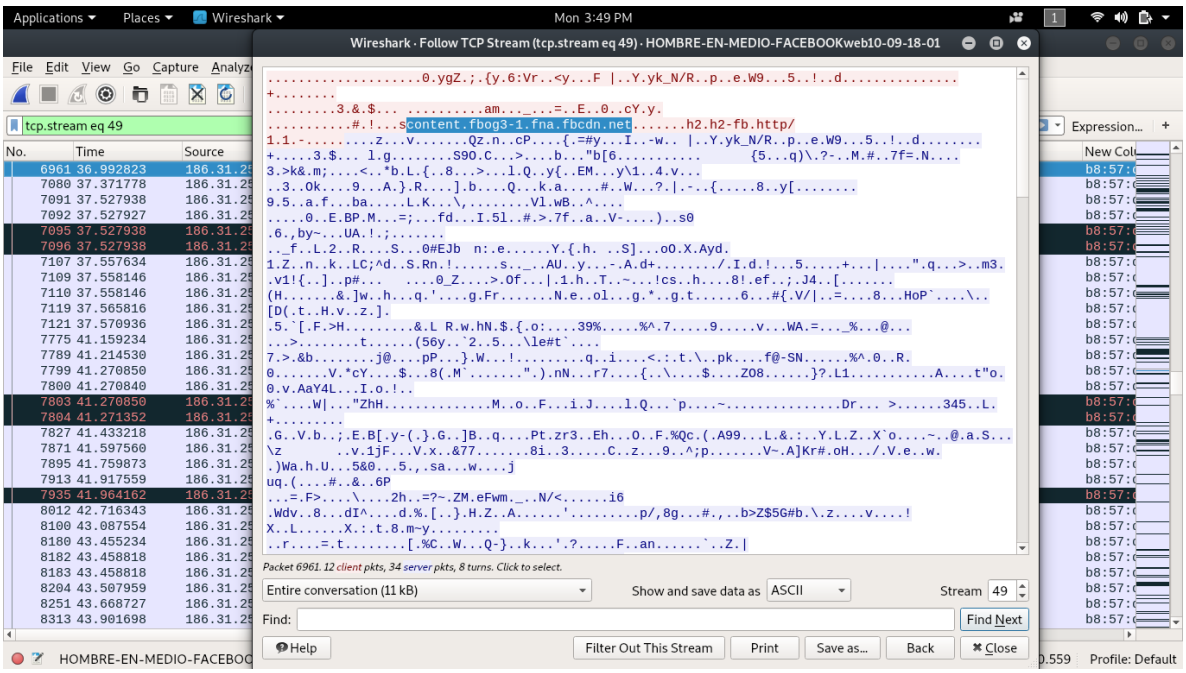


Figura 13.- tráfico cifrado de servidor en Bogotá

Lo cual indica 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, está generando u obteniendo tráfico a través de la aplicación de Facebook.

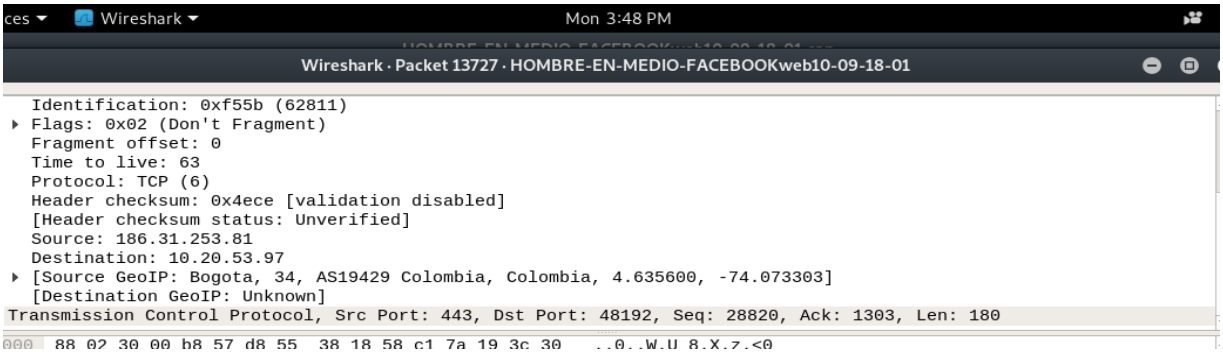


Figura 14.- comunicación relacionada con la IP 168.31.253.81

3.5 Captura - Correo electrónico.

La captura de datos asociados a un correo electrónico se implementó utilizando los servicios de correo que presta Google a través de Gmail. Se capturaron un total de 25.348 paquetes de los cuales 3149 estan asociados al servicio de correo electrónico de Google.

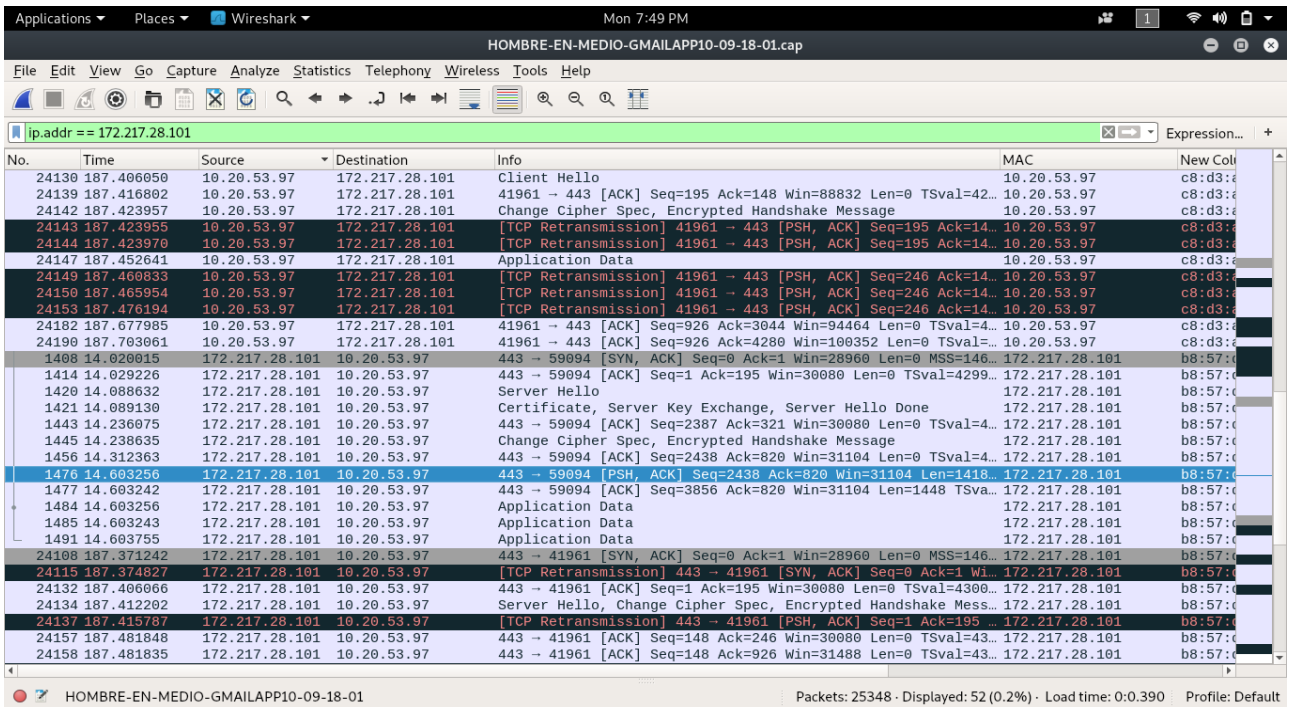


Figura 15.- Captura de datos Gmail

Se identificó que los servidores que responden a las peticiones se encuentran ubicados dentro del terreno asociado a la NASA. Ver figuras 16 y 17.

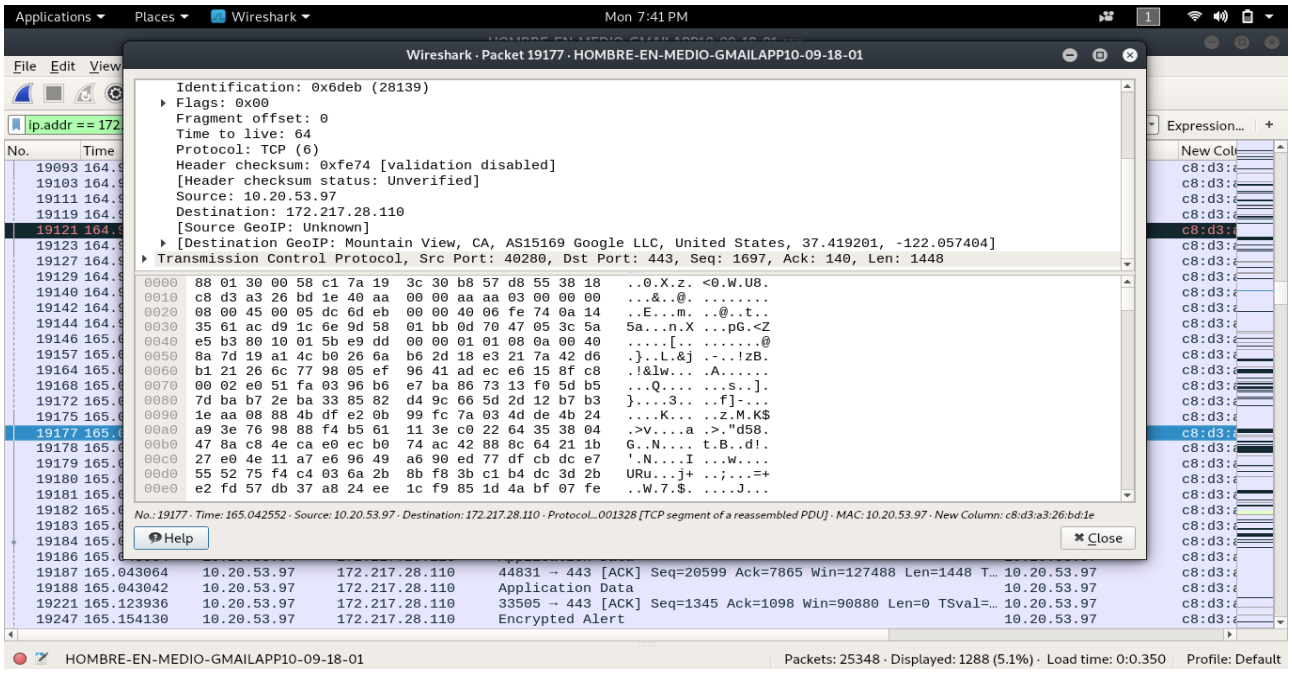


Figura 16.- comunicación relacionada con la IP 172.217.20.210

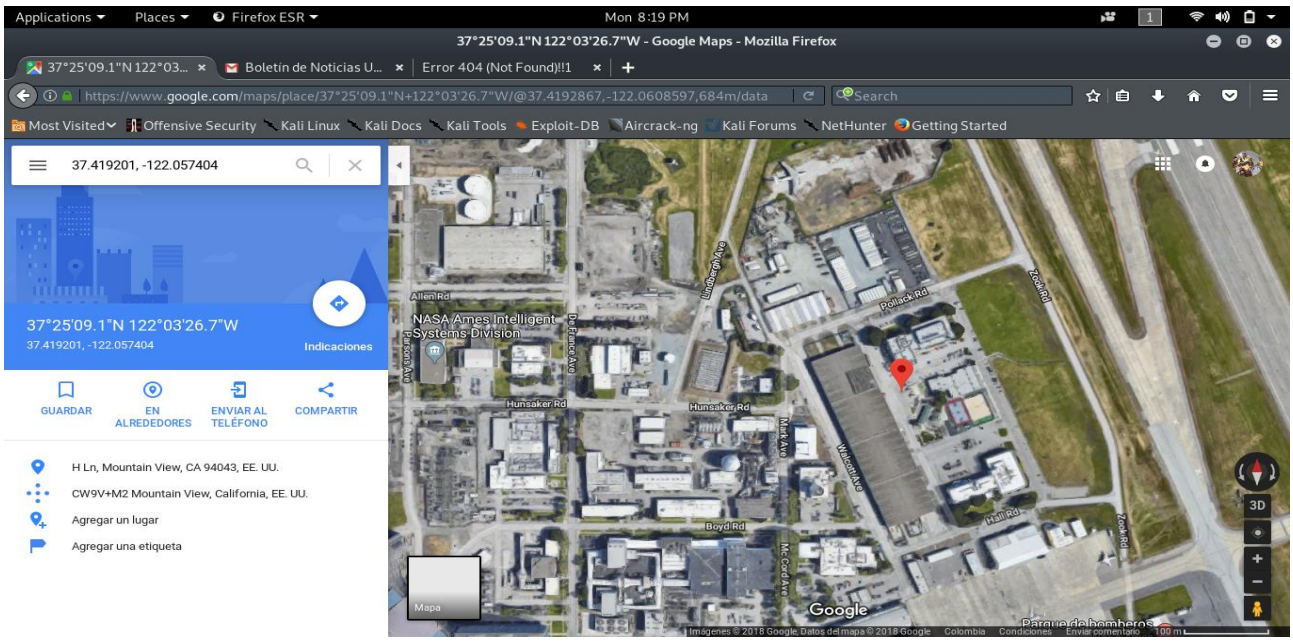


Figura 17.- Ubicación del servidor perteneciente a Google.

En la tabla No 3 se presenta la información de las direcciones IP públicas utilizadas en el proceso de comunicación.

Tabla 3. Estadística de paquetes capturados – correo electrónico

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%

Dentro de la captura se identifica que el 100% de los paquetes asociados al tráfico generado por el consumo de correo electrónico se encuentran cifrados.



Figura 18.- tráfico cifrado relacionado con Gmail

3.6 Uso de VPN

Se implementó una VPN como mecanismo de seguridad al navegar en redes abiertas y se realizó una nueva captura de datos sobre el portal de aulas virtuales de la Universitaria Agustiniana, el cual en pruebas anteriores enviaba la información en texto plano. Al revisar la nueva captura de datos se identificó que el nuevo tráfico se encuentra cifrado.

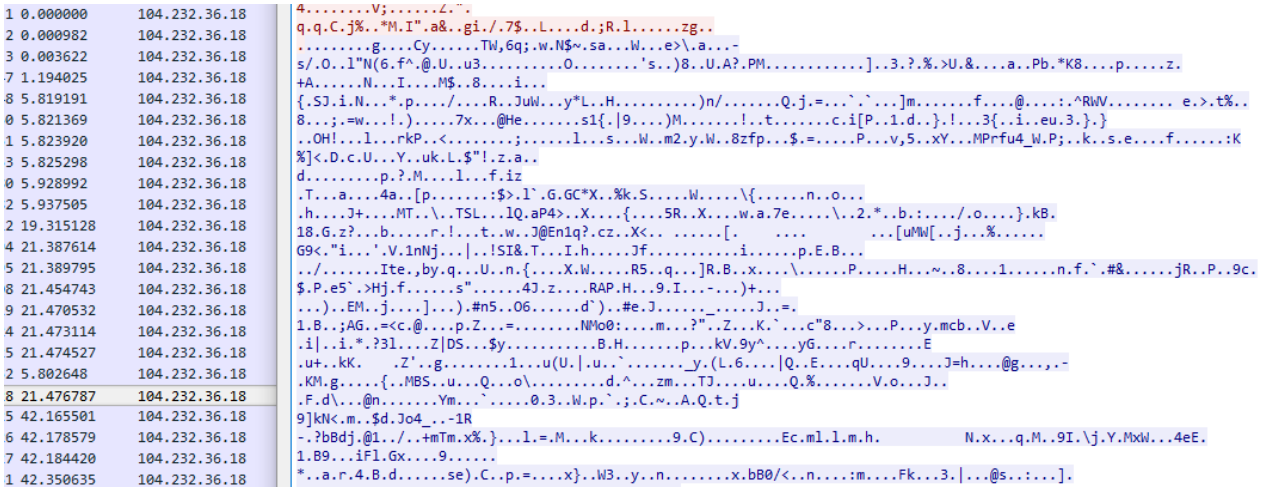


Figura 19.- tráfico cifrado por VPN

3.7 Resumen de resultados

En la tabla No 4 se presenta el resumen de los resultados según las pruebas realizadas en cada una de las aplicaciones WEB

Tabla 4. Resumen de resultados

Nombre de la prueba	Técnica de ataque realizada	Duración de la prueba (minutos de captura de información)	Trafico Cifrado?	Observaciones
Hombre en medio Aulas Virtuales	Hombre en medio	0:03:00	NO	El trafico se trasmite en texto plano 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
Hombre en medio Biblioteca Virtual	Hombre en medio	0:03:00	NO	El tráfico se trasmite sin cifrar lo que permite la captura de información (usuario y contraseña)
Hombre en medio Facebook	Hombre en medio	0:03:00	SI	El tráfico se encuentra cifrado y cumple con los estándares básicos de seguridad, se encontró un tipo de desvío de tráfico hacia 2 direcciones IP sin ninguna asociación hacia Facebook.
Hombre en medio Gmail	Hombre en medio	0:03:00	SI	El tráfico se envía cifrado, previniendo el robo de credenciales de acceso.

Nombre de la prueba	Técnica de ataque realizada	Duración de la prueba (minutos de captura de información)	Trafico Cifrado?	Observaciones
Hombre en medio WhatsApp	Hombre en medio	0:03:00	SI	El tráfico 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.

4. CONCLUSIONES

Se observa que las redes WIFI abiertas presentan una vulnerabilidad al no cifrar la información que se envía a través de estas, relegando la obligación de garantizar la confidencialidad de la información a protocolos establecidos en capas superiores, en otras palabras la confidencialidad de la información depende de medidas tomadas por el servicio WEB que sea consultado por el usuario de la red.

Se encontró que servicios prestados por la Universitaria Uniagustiniana, son susceptibles de ataques tipo MITM al ser consultados desde una red WIFI abierta.

Se evidencia que servicios WEB que cifran en la capa de aplicación la data, aun pueden proveer a los atacantes información valiosa relacionada con la geolocalización de sus servidores.

Se identificó que populares servicios WEB utilizan servidores fantasmas como medida de seguridad que impide el conocer la ubicación física real de sus servidores.

Se pudo comprobar la efectividad de una VPN como medida que garantice la confidencialidad de los datos aun en entornos vulnerables, como lo son las redes WIFI abiertas cuando se navega o consulta servicios que no usan ningún protocolo para el cifrado de la información.

5. REFERENCIAS

[1] B. Sriram and M. A. Sarrayrih, "An analytical study on user satisfaction on Wi-Fi services: A case study on Omani undergraduate environment," *Indian J. Sci. Technol.*, vol. 9, no. 9, 2016.

[2] F. Valle, "Estudio de usos y riesgos asociados a las redes abiertas bajo el protocolo IEEE 802.11 en la ciudad de Bogotá," in *Desarrollo e Innovación en Ingeniería*, 3rd ed., M. E. Serna, Ed. 2018, pp. 73–80.

[3] N. Gcaza and R. von Solms, "A strategy for a cybersecurity culture: A South African perspective," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 80, no. 1, pp. 1–17, 2017.

[4] N. A. Wahab, M. R. Ahmad, A. A. M. Isa, R. F. Malik, and M. R. M. Esa, "WiFi Temporal Coverage: Analysis of Socio-Economics Influences in Malaysia," in *IOP Conference Series: Earth and Environmental Science*, 2019, vol. 228, no. 1.

[5] E. Donavan, "3 Ways to Combat (Growing) Cyber Threat," *cyber Def. Mag.*, pp. 1–97, 2019.

[6] Symantec, "Informe sobre las amenazas para la seguridad en Internet de 2018 | Symantec MX," 2019.

[7] Eleven Paths, "Informe de tendencias en ciberseguridad 2019," 2019.

[8] C. Wang *et al.*, "Accurate sybil attack detection based on fine-grained physical channel information," *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–23, 2018.

[9] M. Gajewski, J. M. Batalla, G. Mastorakis, and C. X. Mavromoustakis, "A distributed IDS architecture model for Smart Home systems," *Cluster Computing*, Springer US, pp. 1–11, 2017.

[10] M. Waliullah, A. B. M. Moniruzzaman, and M. S. Rahman, "An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network," *Int. J. Futur. Gener. Commun. Netw.*, vol. 8, no. 1, pp. 9–18, 2015.

[11] J. Zhang *et al.*, "Defeat Your Enemy Hiding behind Public WiFi: WiGuard Can Protect Your Sensitive Information from CSI-Based Attack," *Appl. Sci.*, vol. 8, no. 4, p. 515, 2018.

[12] J. Milliken, V. Selis, and A. Marshall, "Detection and analysis of the Chameleon WiFi access point virus," *EURASIP J. Inf. Secur.*, vol. 2013, no. 1, p. 2, 2013.

[13] A. Bartoli, E. Medvet, and F. Onesti, “Evil twins and WPA2 Enterprise: A coming security disaster?,” *Comput. Secur.*, vol. 74, pp. 1–11, 2018.
[14] J. Xiong and K. Jamieson, “SecureArray: improving wifi security with fine-grained physical-layer information,” in *Proceedings of the 19th annual international conference on Mobile computing & networking - MobiCom ’13*, 2013, p. 441.
[15] K. K. K. Fong and S. K. S. Wong, “Wi-Fi adoption and security in Hong Kong,” *Asian Soc. Sci.*, vol. 12, no. 6, pp. 1–22, 2016.
[16] J. S. Atkinson, J. E. Mitchell, M. Rio, and G. Matich, “Your WiFi is leaking: What do your mobile apps gossip about you?,” *Futur. Gener. Comput. Syst.*, vol. 80, pp. 546–557, 2018.
[17] B. Naeem, U. A. K. Chude-Okonkwo, R. Ngah, S. Z. M. Hashim, W. Maqboo, and S. Hashim, “Exploring the open problems and future trends concerning handovers in heterogeneous wireless networks: A review,” *J. Teknol.*, vol. 3, no. 3, pp. 13–17, 2014.
[18] C. Chilipirea, M. Baratchi, C. Dobre, and M. van Steen, “Identifying stops and moves in WiFi tracking data,” *Sensors (Switzerland)*, vol. 18, no. 11, pp. 1–15, 2018.
[19] X. Guo and P. Xia, “Mine personnel location system based on Internet of things,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 439, no. 3, 2018.
[20] T. Melamed, “An active man-in-The-middle attack on bluetooth smart devices,” in *International Journal of Safety and Security Engineering*, 2018, vol. 8, no. 2, pp. 200–211.
[21] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, “Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN),” *J. Comput. Networks Commun.*, vol. 2019, pp. 1–14, 2019.
[22] E. P. Lane, “Neither Snow Nor Rain Nor MITM . . . An Empirical Analysis of Email Delivery Security,” pp. 281–296, 2015.
[23] F. Aliyu, T. Sheltami, and E. M. Shakshuki, “A detection and prevention technique for man in the middle attack in fog computing,” in *Procedia Computer Science*, 2018, vol. 141, pp. 24–31.