

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.

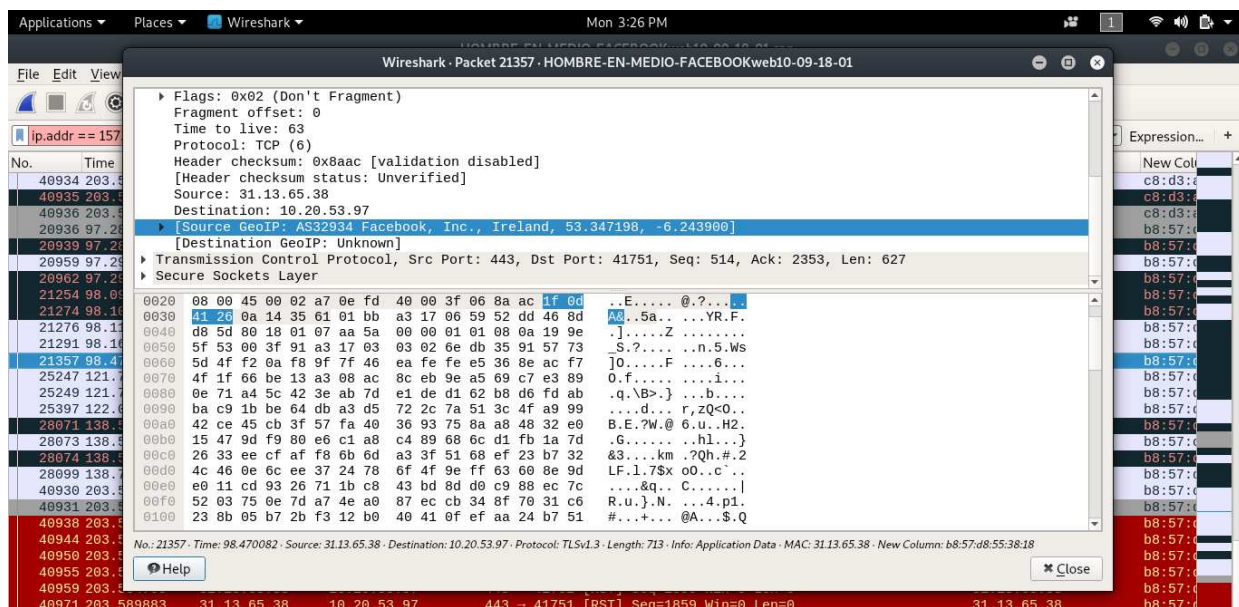


Figura 37 Paquetes capturados desde los servicios de Facebook con parámetros de geolocalización.

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

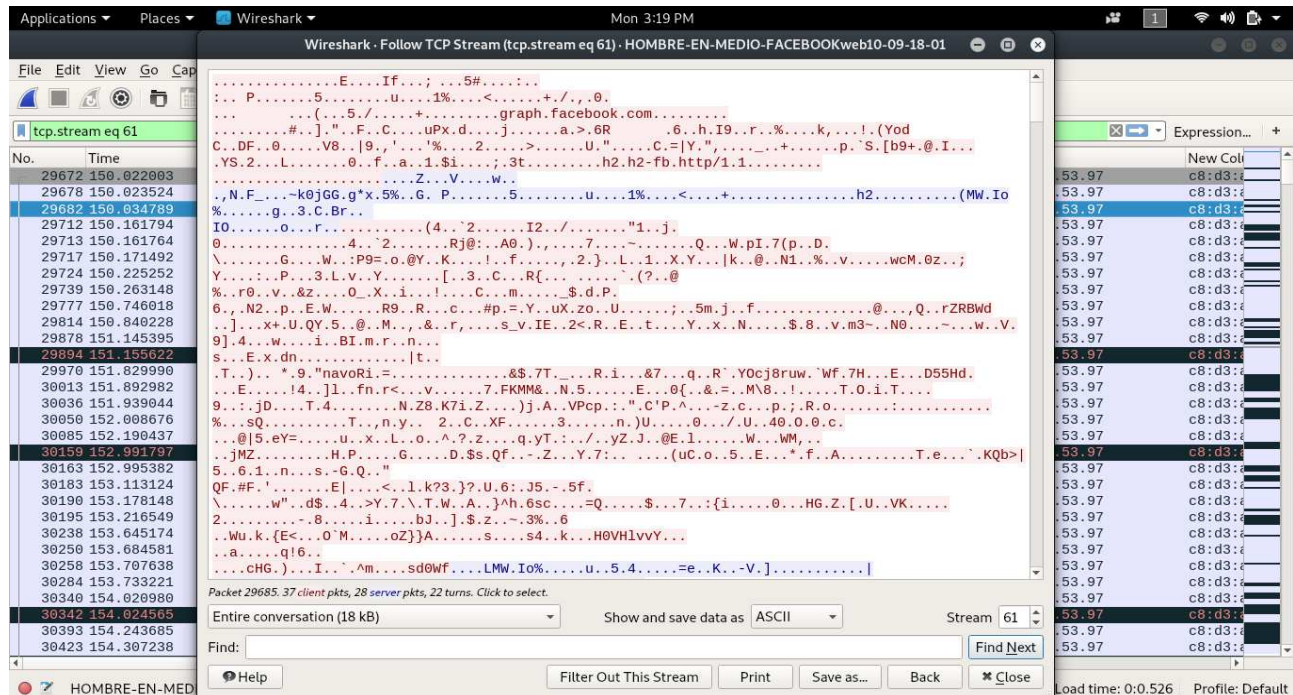


Figura 38 Paquetes capturados desde los servicios de Facebook evidenciando su total encriptación

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

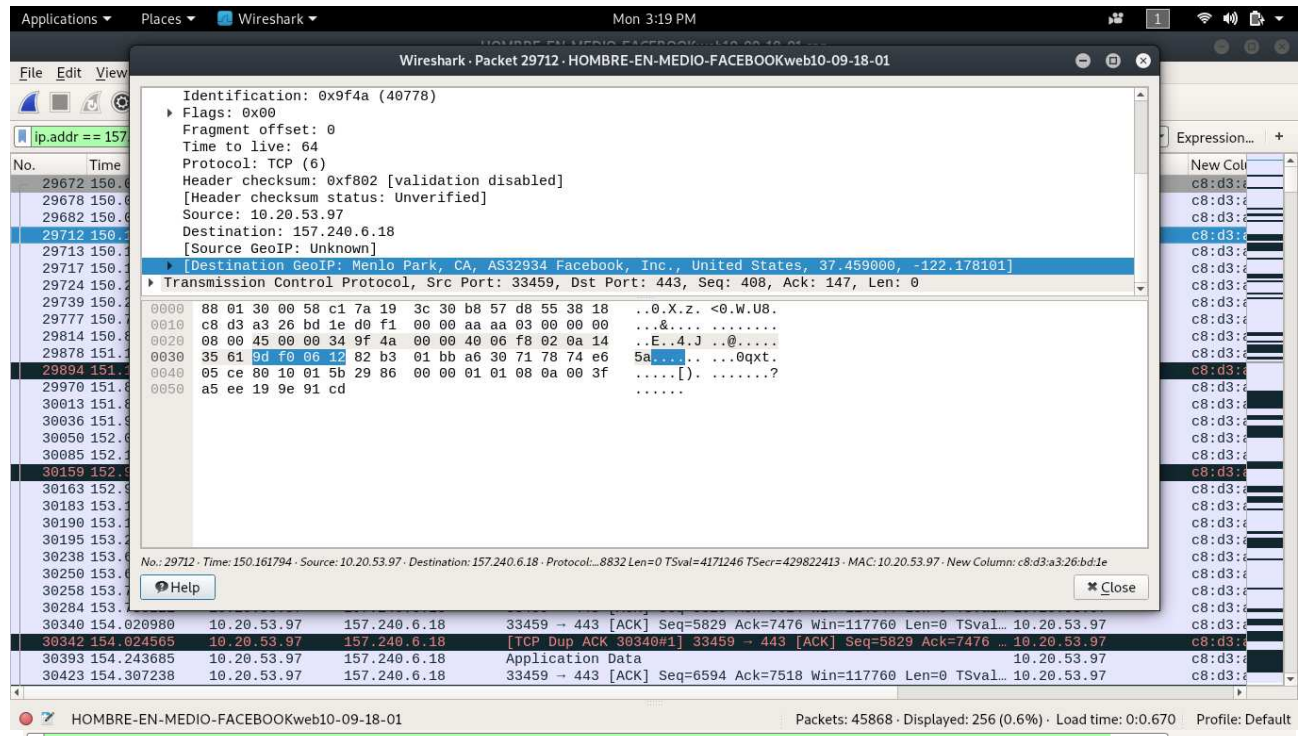


Figura 40 Paquetes capturados desde los servicios de Facebook con valores de GeoIP

No.	Time	Source	Destination	Protocol	Length	Info	GeoIP
31055	169.998712	10.20.53.97	157.240.6.18	Application Data		10.20.53.97	c8:d3:...
31696	161.107509	10.20.53.97	157.240.6.18	Application Data		10.20.53.97	c8:d3:...
31835	161.672309	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=13424 Ack=25038 Win=167168 Len=0 TSV...		10.20.53.97	c8:d3:...
31859	161.799777	10.20.53.97	157.240.6.18	[TCP ACKed unseen segment] 33459 → 443 [ACK] Seq=13424 Ack...		10.20.53.97	c8:d3:...
32652	165.877692	10.20.53.97	157.240.6.18	[TCP ACKed unseen segment] 33459 → 443 [ACK] Seq=13424 Ack...		10.20.53.97	c8:d3:...
32713	166.063477	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=13424 Ack=28998 Win=175616 Len=0 Tsv...		10.20.53.97	c8:d3:...
32787	166.291871	10.20.53.97	157.240.6.18	[TCP Previous segment not captured], Application Data		10.20.53.97	c8:d3:...
32839	166.494111	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=29744 Win=181248 Len=0 Tsv...		10.20.53.97	c8:d3:...
32860	166.624159	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=30256 Win=184320 Len=0 Tsv...		10.20.53.97	c8:d3:...
32875	166.628277	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=31764 Win=187136 Len=0 Tsv...		10.20.53.97	c8:d3:...
32877	166.628277	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=32028 Win=189952 Len=0 Tsv...		10.20.53.97	c8:d3:...
32929	166.751156	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=32540 Win=193024 Len=0 Tsv...		10.20.53.97	c8:d3:...
32930	166.751170	10.20.53.97	157.240.6.18	[TCP Dup ACK 32929#1] 33459 → 443 [ACK] Seq=14408 Ack=3254...		10.20.53.97	c8:d3:...
32932	166.751157	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=33052 Win=195840 Len=0 Tsv...		10.20.53.97	c8:d3:...
32940	166.751682	10.20.53.97	157.240.6.18	[TCP Dup ACK 32932#1] 33459 → 443 [ACK] Seq=14408 Ack=3305...		10.20.53.97	c8:d3:...
32945	166.751682	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=33564 Win=198656 Len=0 Tsv...		10.20.53.97	c8:d3:...
32956	166.751647	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=34076 Win=201728 Len=0 Tsv...		10.20.53.97	c8:d3:...
32965	166.806429	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=35100 Win=204544 Len=0 Tsv...		10.20.53.97	c8:d3:...
33070	167.173555	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=35612 Win=207360 Len=0 Tsv...		10.20.53.97	c8:d3:...
33094	167.233972	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=36636 Win=210432 Len=0 Tsv...		10.20.53.97	c8:d3:...
33132	167.390210	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=38596 Win=216064 Len=0 Tsv...		10.20.53.97	c8:d3:...
33133	167.390176	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=38684 Win=216064 Len=0 Tsv...		10.20.53.97	c8:d3:...
33571	168.585770	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=40644 Win=221952 Len=0 Tsv...		10.20.53.97	c8:d3:...
33573	168.585769	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=40732 Win=221952 Len=0 Tsv...		10.20.53.97	c8:d3:...
33613	168.699458	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=41244 Win=224768 Len=0 Tsv...		10.20.53.97	c8:d3:...
33614	168.699458	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=41756 Win=227584 Len=0 Tsv...		10.20.53.97	c8:d3:...
33679	168.795691	10.20.53.97	157.240.6.18	33459 → 443 [ACK] Seq=14408 Ack=43204 Win=230656 Len=0 Tsv...		10.20.53.97	c8:d3:...

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.

No.	Time	Source	Destination	Info	MAC	New Col
31359	160.100852	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=7555 Win=123392 Len=0 TSval...	10.20.53.97	c8:d3:
31360	160.100853	10.20.53.97	157.240.6.19	[TCP Dup ACK 31359#1] 34900 → 443 [ACK] Seq=1099 Ack=7555 ...	10.20.53.97	c8:d3:
31381	160.159201	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=7811 Win=126208 Len=0 TSval...	10.20.53.97	c8:d3:
31523	160.598558	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=8835 Win=134656 Len=0 TSval...	10.20.53.97	c8:d3:
31536	160.659598	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=8953 Win=134656 Len=0 TSval...	10.20.53.97	c8:d3:
31541	160.660510	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=9209 Win=137472 Len=0 TSval...	10.20.53.97	c8:d3:
31578	160.727106	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=9465 Win=140288 Len=0 TSval...	10.20.53.97	c8:d3:
31579	160.727092	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=9721 Win=143104 Len=0 TSval...	10.20.53.97	c8:d3:
31622	160.900661	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=10379 Win=145664 Len=0 TSva...	10.20.53.97	c8:d3:
31641	160.965684	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=10891 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32178	163.720437	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=10955 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32253	164.010742	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11055 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32269	164.072672	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11091 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32302	164.193525	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11219 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32351	164.482869	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11327 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32372	164.544289	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11363 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32377	164.550452	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11399 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32384	164.608309	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11403 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32388	164.615456	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11439 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32414	164.673333	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11511 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32455	164.803996	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11521 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32468	164.818741	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11629 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32505	164.947747	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11773 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32628	165.751170	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11917 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32629	165.751157	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=11953 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:
32648	165.871457	10.20.53.97	157.240.6.19	34900 → 443 [ACK] Seq=1099 Ack=12097 Win=148480 Len=0 TSva...	10.20.53.97	c8:d3:

Figura 41 Paquetes capturados desde los servicios de Facebook

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

Wireshark - Follow TCP Stream (tcp.stream eq 67) - HOMBRE-EN-MEDIO-FACEBOOKweb10-09-18-01

```

.....t@.}>.t.No..dh.*.d5x".W.]...&4..+.4.6.....+./.,.0.
.....(.5./.....+.video.xx.fbcdn.net.....
.....#..].".
Ava..m..Zd"...].6...\.G3...S.Ms..D[...C.%..xj...!@...=-.qw.
.....73...1..CWkn...41..SKw.)-..yI...1...u...=...+jVq2...).
2.....u...u..Xyod.B.aol]...e.....M;.....p.v.3t.....h2.h2-fb.http/1.1.....
.....Z..V.....D.....F.....1.....r+
.....&4..+.4.6.....+.h2.....
[&Hc*...m@...n..w..X...K.Vr.i.r".e.....(F
$=#./Yc.D.Z...S2.fy.c...b.N.....UF$=#./...z...=.7#>.....c.u...0.&...6..A.".
42.S.jsN.e$).l.z.<@Vm...cp.S.6vf.h.=>.R..h...Thtg...V.m9...j..8.P.....m.f...=...Q;
+*]X(...S.O...
YP.eP..z...L.....?..WcX...&.....pRm.NNF.V.E...M.....A.....<V...U...=#
v.$)...i...x.u..J...N
.D.X...m..X+N{.....I.d.5.ty.:&...e.m
*...h).J..3.3...y.Z...3k...q...I..I.
.....um].7..h..F.]>.6.....h.C.....l..n..V;.....<...T...+..$K...".0...<.g...}C..6..
(./+/{...F&S6s".!i,..Ht
.....Ny.M;...@...
8B.o...!].5.p...;...p.G..
V...o...y..=;2;<b9...L...+o.S...K.w.i..sn.(1.jh...L&Hc*...sK...4].6..
e0q..q7r..N...if.K.(.A.r..n!..1.Pv..A;..4.....&Hc*.....?.....[...@...@...{.R]
a.....A:\...&Hc*...e.e..8...0
.....]ePLSm...8.e..#
[*2.<A...{...F...s...n...h.h...n
/;...;\X4..F
!..!..AX..T.o.n.QR.....ud].1.\zy...6.L.$..z..w..<.f/...5.r...>0w..B}6..1F.4..d..t...
+@Bfb)c.JW...X.@...N...X...8..$.t..J..d.9<.....3..X.....oIF
$=#./...r..#i.?..AR..0?..C[42 bytes missing in capture file]...2F
$=#./...1...}...1..0...{K..E.%0.[B.1.....%F$=#./...=...nN.>...k...6..

```

Packet 30351: 11 client pkts, 7 server pkts, 6 turns. Click to select.

Entire conversation (1781 bytes) Show and save data as ASCII Stream 67

Find: Find Next

Filter Out This Stream Print Save as... Back Close

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.

No.	Time	Source	Destination	Info	MAC	New Column
40928	201.088565	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=25587 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
40928	201.575520	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=25715 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
40928	202.419870	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=25779 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
40670	202.771637	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=25843 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
40671	202.771638	10.20.53.97	157.240.6.23	[TCP Dup ACK 40670#1] 58730 → 443 [ACK] Seq=1878 Ack=25843...	10.20.53.97	c8:d3:...
40819	203.132597	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=25971 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
41032	203.880671	10.20.53.97	157.240.6.23	[TCP ACKed unseen segment] 58730 → 443 [ACK] Seq=1878 Ack=...	10.20.53.97	c8:d3:...
41278	204.681538	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=26163 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
41280	204.682050	10.20.53.97	157.240.6.23	[TCP Dup ACK 41278#1] 58730 → 443 [ACK] Seq=1878 Ack=26163...	10.20.53.97	c8:d3:...
41377	204.960566	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=26291 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
41940	206.150494	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=26483 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
41942	206.150494	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=26547 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
41944	206.151005	10.20.53.97	157.240.6.23	[TCP Dup ACK 41942#1] 58730 → 443 [ACK] Seq=1878 Ack=26547...	10.20.53.97	c8:d3:...
42117	206.720930	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=26675 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
42118	206.720930	10.20.53.97	157.240.6.23	[TCP Dup ACK 42117#1] 58730 → 443 [ACK] Seq=1878 Ack=26675...	10.20.53.97	c8:d3:...
42550	208.736821	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=26739 Win=155136 Len=0 TSva...	10.20.53.97	c8:d3:...
42590	208.920117	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=27187 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
43159	210.675380	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=27251 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
43160	210.675381	10.20.53.97	157.240.6.23	[TCP Dup ACK 43159#1] 58730 → 443 [ACK] Seq=1878 Ack=27251...	10.20.53.97	c8:d3:...
43307	211.048085	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=27507 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
43741	213.312372	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=1878 Ack=27763 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
43870	213.693812	10.20.53.97	157.240.6.23	Application Data	10.20.53.97	c8:d3:...
43918	213.806964	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=2163 Ack=27827 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
44175	214.806428	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=2163 Ack=27891 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
44866	217.549840	10.20.53.97	157.240.6.23	[TCP Previous segment not captured] 58730 → 443 [ACK] Seq=...	10.20.53.97	c8:d3:...
45307	219.404537	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=2627 Ack=28211 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
45308	219.404515	10.20.53.97	157.240.6.23	[TCP Dup ACK 45307#1] 58730 → 443 [ACK] Seq=2627 Ack=28211...	10.20.53.97	c8:d3:...
45436	220.194026	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=2627 Ack=28239 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
45586	221.090082	10.20.53.97	157.240.6.23	58730 → 443 [ACK] Seq=2627 Ack=28303 Win=157952 Len=0 TSva...	10.20.53.97	c8:d3:...
45599	221.095714	10.20.53.97	157.240.6.23	[TCP Dup ACK 45586#1] 58730 → 443 [ACK] Seq=2627 Ack=28303...	10.20.53.97	c8:d3:...

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

Protocol: TCP (v)

Header checksum: 0xd3c2 [validation disabled]

[Header checksum status: Unverified]

Source: 10.20.53.97

Destination: 157.240.6.19

[Source GeoIP: Unknown]

Destination GeoIP: Menlo Park, CA, AS32934 Facebook, Inc., United States, 37.459000, -122.178101

Transmission Control Protocol, Src Port: 34900, **Dst Port:** 443, **Seq:** 1099, **Ack:** 11327, **Len:** 0

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

Entire conversation (3838 bytes)

 Show and save data as ASCII

 Stream 66

Figura 45 Paquetes capturados evidenciando su total encriptación

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

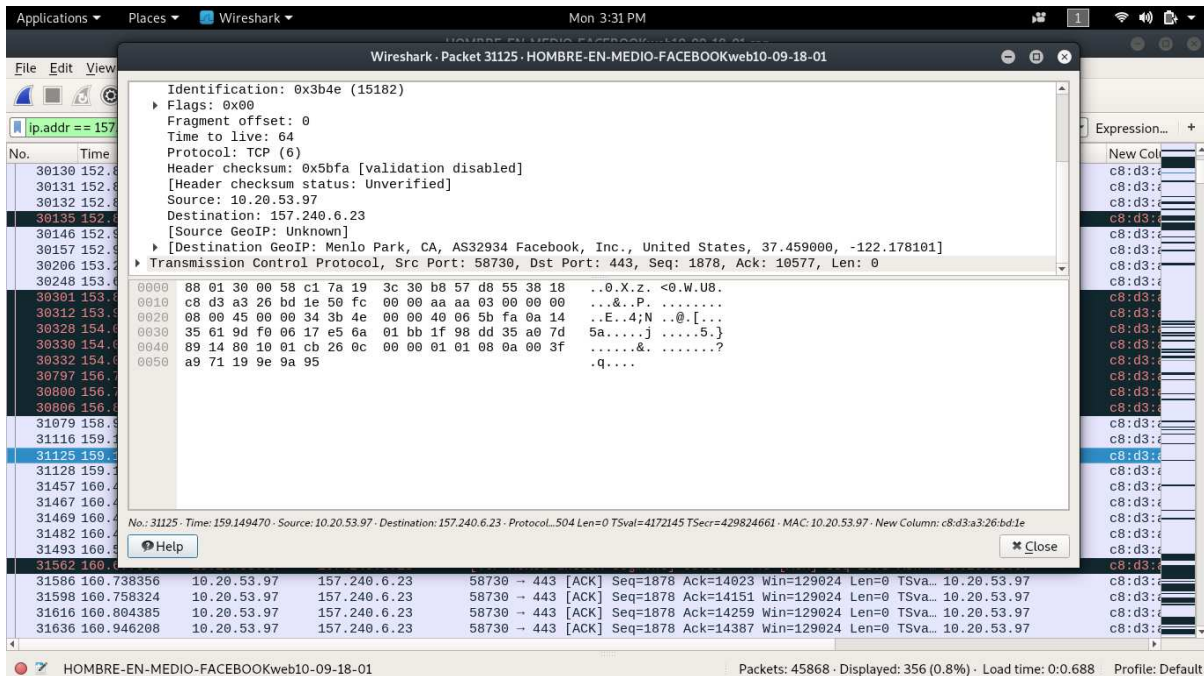


Figura 46 Paquetes capturados desde los servicios de Facebook con valores de GeoIP

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.

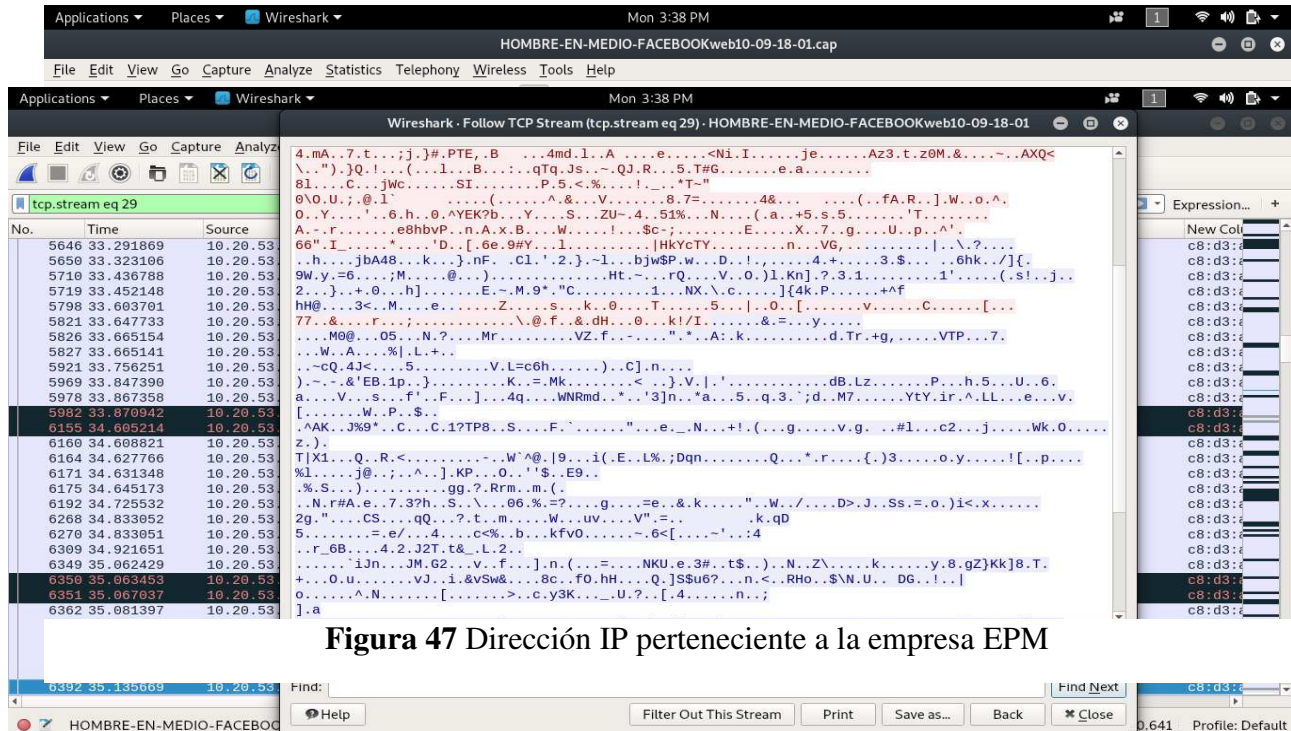


Figura 47 Dirección IP perteneciente a la empresa EPM

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.

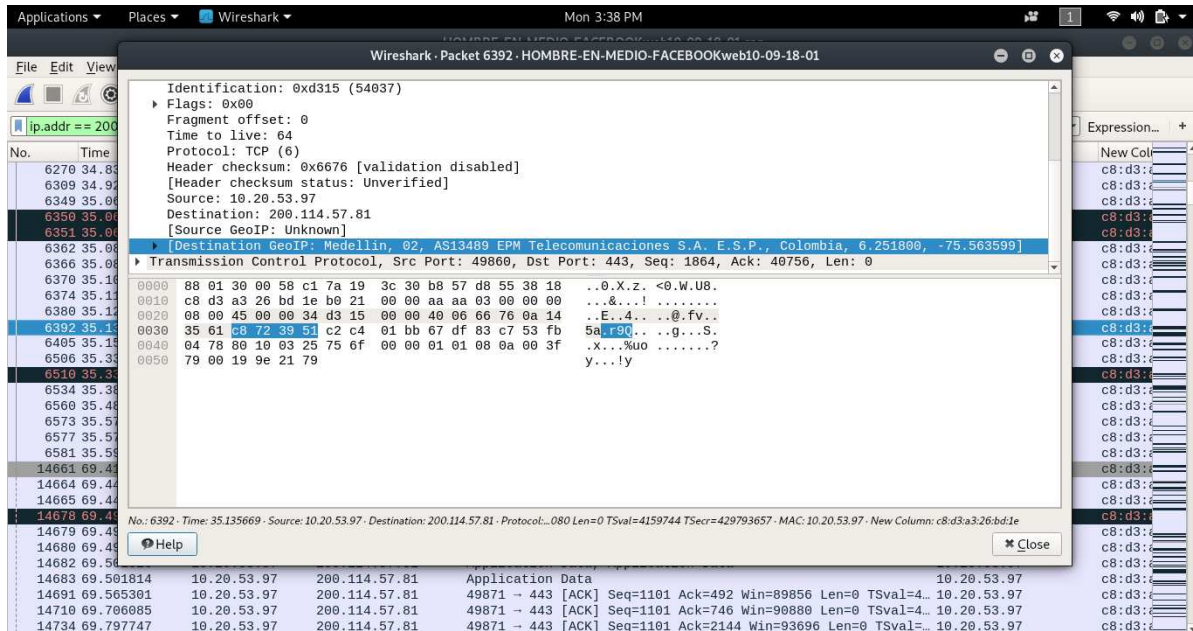


Figura 49 Paquetes capturados de la empresa EPM con su geolocalización

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.

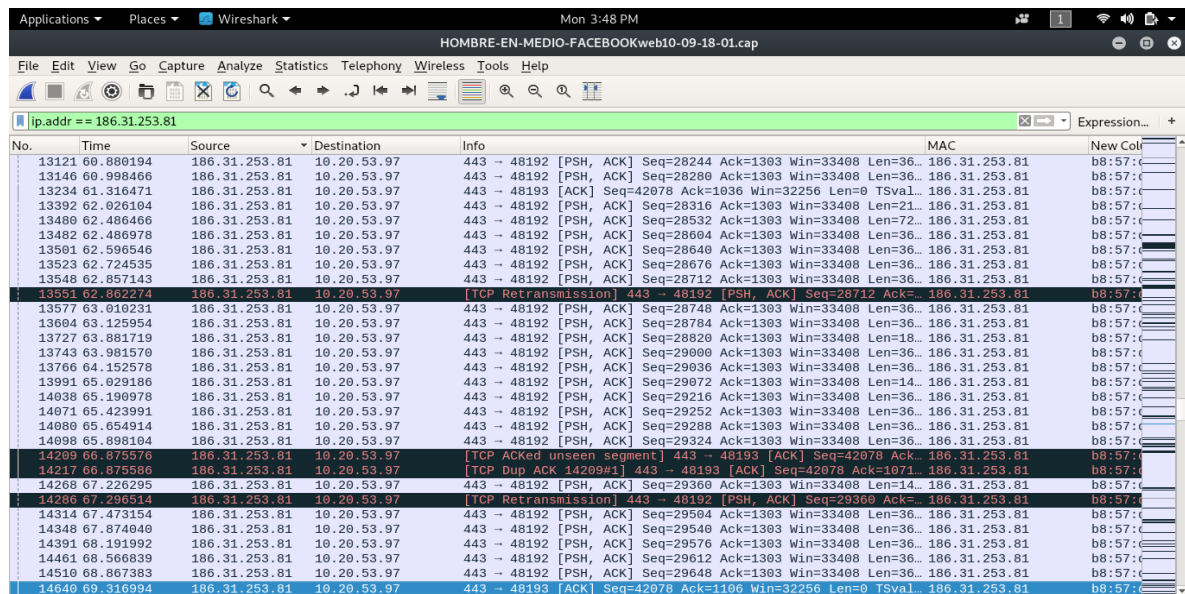


Figura 50 Paquetes capturados generando tráfico significativo con la IP 186.31.253.81

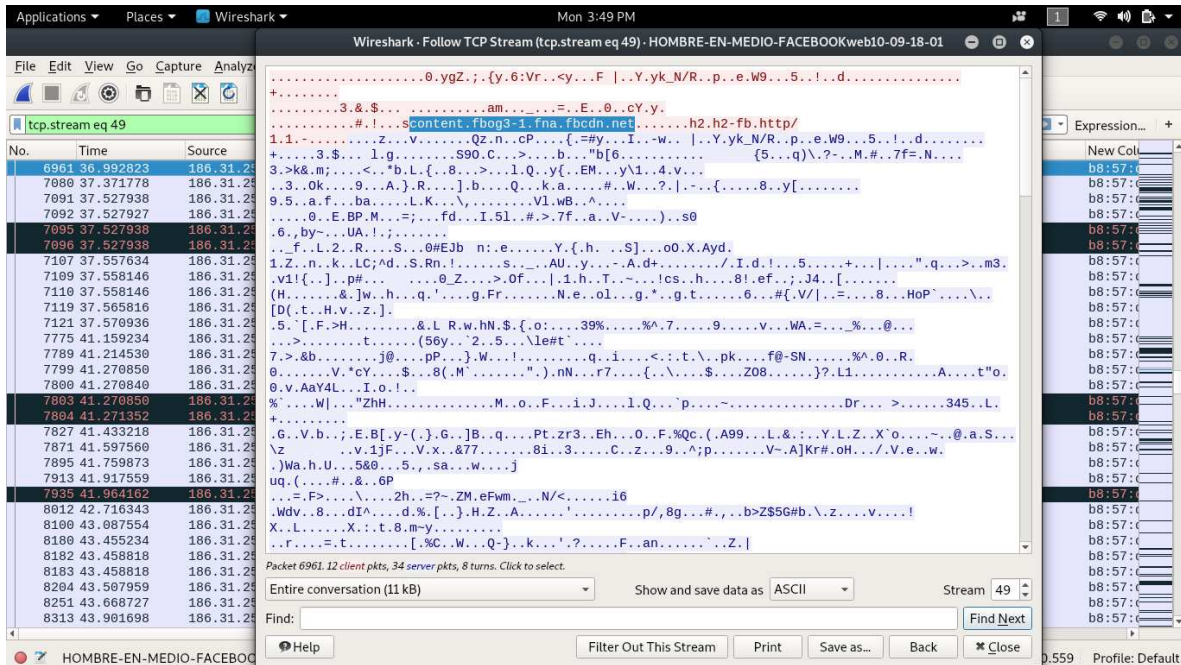


Figura 51 Paquetes capturados encriptados con encabezados de Facebook

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.

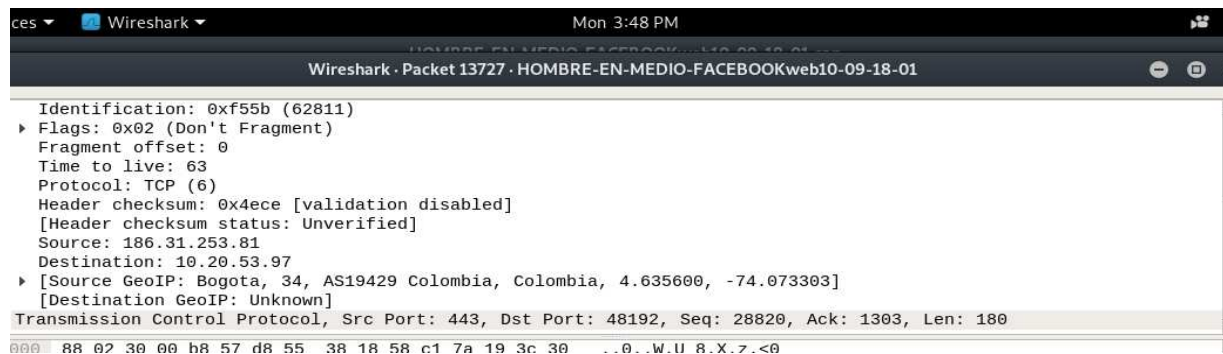


Figura 52 Paquetes capturados con geolocalización en Bogotá

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.

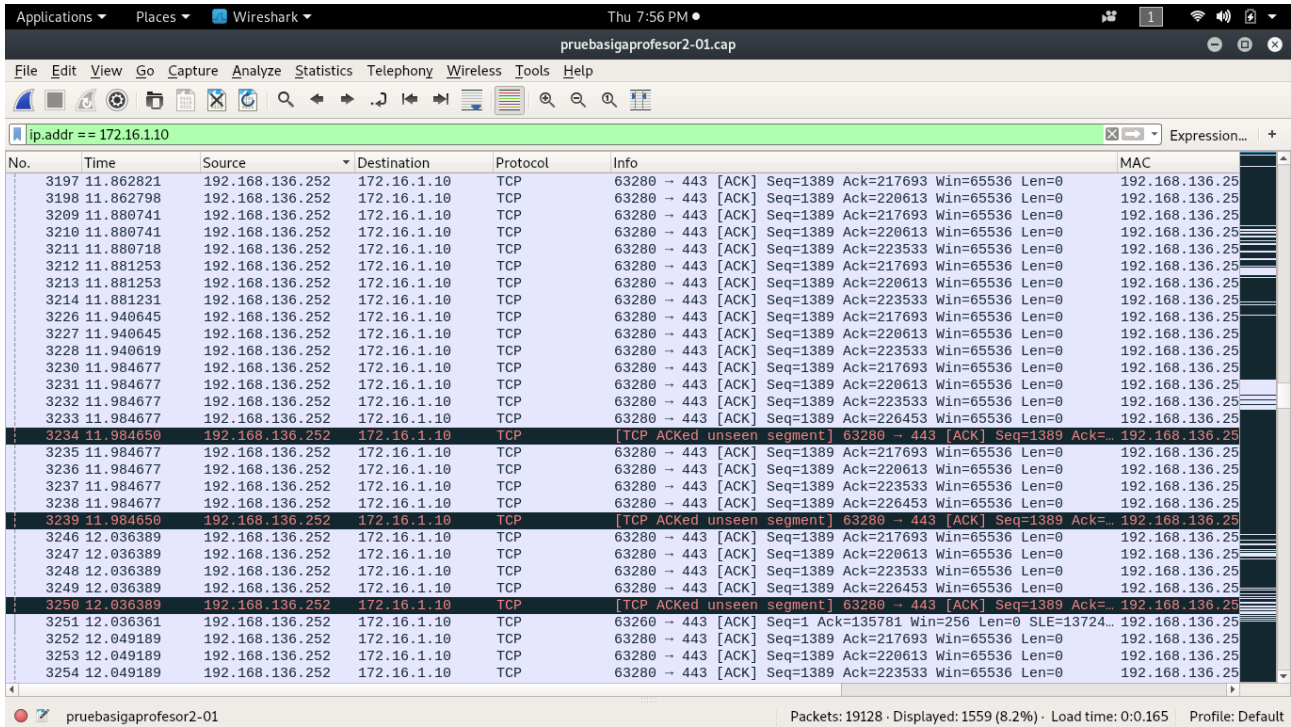


Figura 54 Trafico capturado del servicio del siga

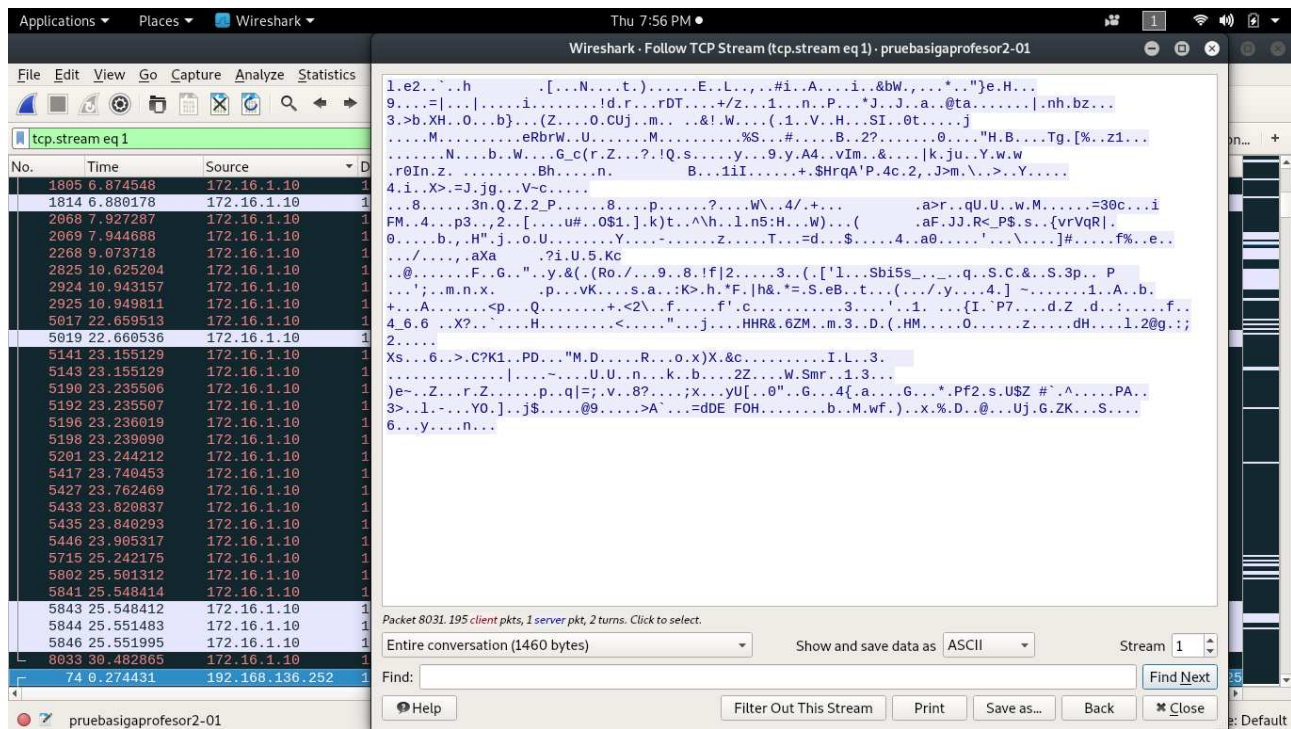


Figura 53 Trafico capturado del siga totalmente cifrado

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 Agustiniiana, 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 55Tráfico encriptado de la VPN

El aplicativo cambia la dirección IP que responde de 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

Figura 1 Diagrama de redes inalámbricas (katheryne; & romero, 2012).....	14
Figura 2 Generalidades de protocolos de seguridad (Ciens, s.f.).....	15
Figura 3 Uso de los protocolos de encriptación (Websec, 2013).....	16
Figura 4 Cronograma de actividades.....	24
Figura 5 Proceso de captura de tráfico sobre SSID “VIRUS-NO-CONECTAR” para la aplicación de aulas virtuales.	28
Figura 6 Trafico capturado para la prueba aulas virtuales agustinianas	29
Figura 7 Gráficos capturados de las preguntas del simulacro del examen del saber pro 2018	30
Figura 8 Captura de las fotos de identificación en la plataforma de los estudiantes asociados al simulacro del saber PRO 2018	30
Figura 9 Proceso de captura de tráfico sobre SSID “VIRUS-NO-CONECTAR” para la aplicación de la biblioteca virtual.	31
Figura 10 Información capturada del proceso de ingreso a la plataforma.	32
Figura 11 Proceso de captura de tráfico sobre SSID “VIRUS-NO-CONECTAR” para la aplicación WhatsApp.....	33
Figura 12 Valores geológicos de la dirección IP publica 157.240.14.53.....	34
Figura 13 Trafico capturado desde la aplicación de WhatsApp.....	34
Figura 14 Trafico analizado desde la aplicación de WhatsApp.....	35
Figura 15 Proceso de captura de tráfico sobre SSID “VIRUS-NO-CONECTAR” para la aplicación WhatsApp.....	36
Figura 16 Ubicación geográfica de los servidores pertenecientes a servicios de Google.....	36
Figura 17 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.110	37
Figura 18 Paquete analizado proveniente de los servicios de Google	38
Figura 19 Valores de geolocalización e identificación de la dirección IP 172.217.28.110	38
Figura 20 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.101	39
Figura 21 Paquete analizado proveniente de la dirección IP 172.217.28.101	39
Figura 22 Valores de geolocalización e identificación de la dirección IP 172.217.28.101	40
Figura 23 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.109	40
Figura 24 Paquetes analizados proveniente de la dirección IP 172.217.28.109	41

Figura 25 Valores de geolocalización e identificación de la dirección IP 172.217.28.109	42
Figura 26 Paquetes capturados desde los servicios de Google con dirección IP 172.217.28.99	42
Figura 27 Paquetes analizados provenientes desde la dirección IP 172.217.28.99	43
Figura 28 Paquetes capturados desde los servicios de Google y su geolocalización.....	43
Figura 29 Paquetes capturados con dirección IP 216.58.222.202.....	44
Figura 30 Evidencia de trafico cifrado desde la dirección IP 216.58.222.202	44
Figura 31 Paquetes capturados desde los servidores de Google con su geolocalización en protocolo IPV4	45
Figura 32 Paquetes capturados desde los servicios de Facebook con dirección IP 31.13.65.7	47
Figura 33 Paquetes capturados desde los servicios de Facebook validando que se encuentra la información encriptada.....	47
Figura 34 Paquetes capturados desde los servicios de Facebook con su geolocalización	48
Figura 35 Paquetes capturados desde los servicios de Facebook que responde a la IP 31.13.65.38 .	48
Figura 36 Paquetes capturados desde los servicios de Facebook.....	49
Figura 37 Paquetes capturados desde los servicios de Facebook con parámetros de geolocalización.	49
Figura 38 Paquetes capturados desde los servicios de Facebook evidenciando su total encriptación	50
Figura 39 Paquetes capturados desde los servicios de Facebook respondiendo a la IP 157.240.6.18	51
Figura 40 Paquetes capturados desde los servicios de Facebook con valores de GeoIP	51
Figura 41 Paquetes capturados desde los servicios de Facebook.....	52
Figura 42 Paquetes capturados desde los servicios de Facebook evidenciando su cifrado	52
Figura 43 Paquetes capturados desde los servicios de Facebook con valores de GeoIP	53
Figura 44 Paquetes capturados desde los servicios de Facebook respondiendo a la IP 157.240.6.23	53
Figura 45 Paquetes capturados evidenciando su total encriptación	53
Figura 46 Paquetes capturados desde los servicios de Facebook con valores de GeoIP	54
Figura 47 Dirección IP perteneciente a la empresa EPM.....	55
Figura 48 Trafico capturado de la IP de la empresa de EPM.....	55
Figura 49 Paquetes capturados de la empresa EPM con su geolocalización	56
Figura 50 Paquetes capturados generando tráfico significativo con la IP 186.31.253.81.....	56

Figura 51 Paquetes capturados encriptados con encabezados de Facebook	57
Figura 52 Paquetes capturados con geolocalización en Bogotá.....	57
Figura 53 Trafico capturado del siga totalmente cifrado	59
Figura 54 Trafico capturado del servicio del siga	59
Figura 55 Trafico encriptado de la VPN	62

13. Lista de tablas

Tabla 1	17
Tabla 2	21
Tabla 3	23
Tabla 4	25
Tabla 5	26
Tabla 6	26
Tabla 7	27
Tabla 8	29
Tabla 9	32
Tabla 10	37
Tabla 11	46
Tabla 12	58

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