به نام خدا

محمدمهدی آقاجانی

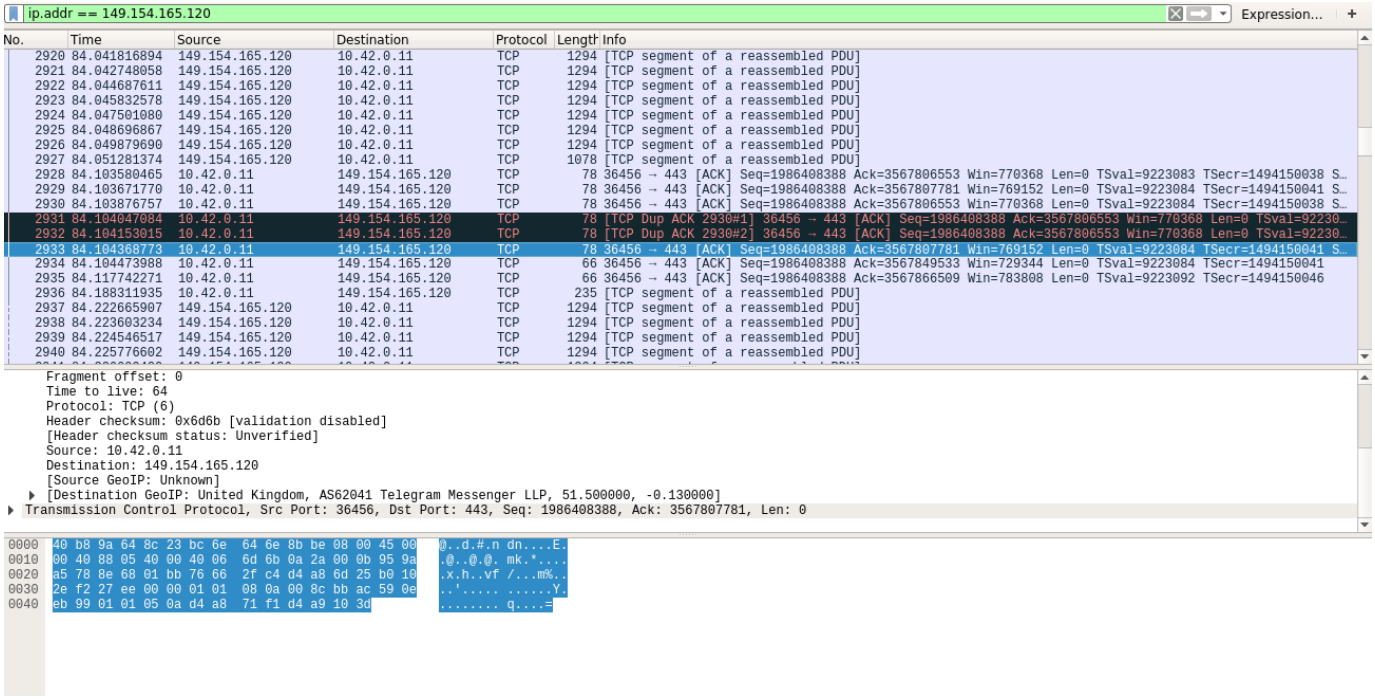
۹۳۳۱۰۵۶

تمرین عملی اول

استاد : دکتر شهریاری

سؤال اول

پروتکل های مورد استفاده بیشتر ssl , sslv2 , tcp می‌باشد



.بسته های رد و بدل شده تماماً رمز شده می باشند.

یک نکته مشهود این می‌باشد که تلگرام چندین سرور مختلف دارد که در هر بار اتصال به یکی از .آن‌ها متصل می‌شود

همچنین برای ارسال داده‌ها از پروتکلssl استفاده میکند تا داده‌ها رمز شده باقی بمانند.

سؤال دوم

بخش اول)

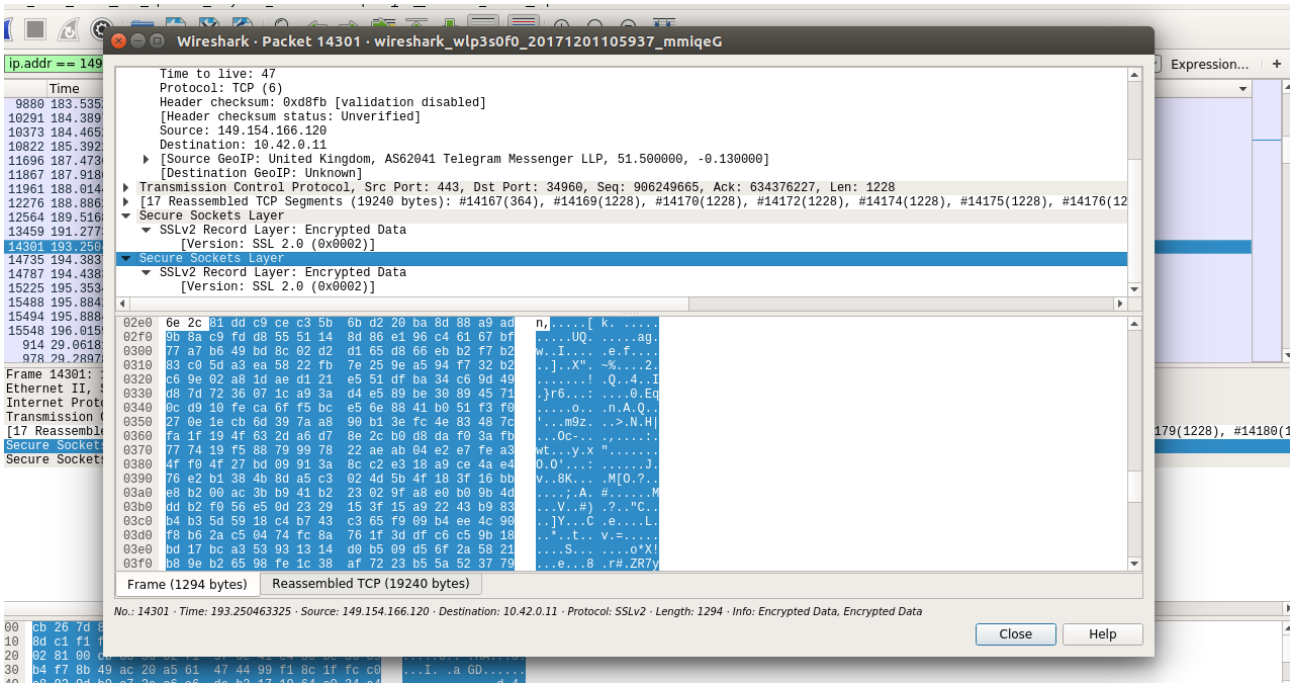
91.108.4.134

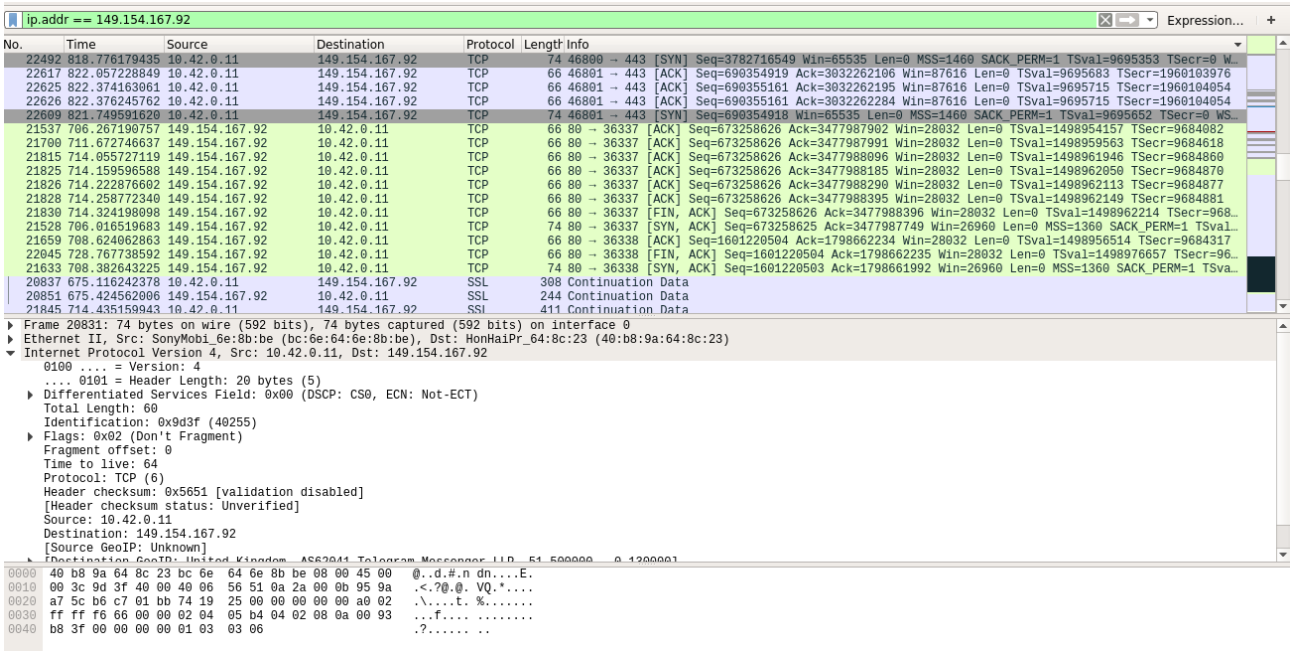
149.154.166.120

149.154.167.92

بخش دوم)

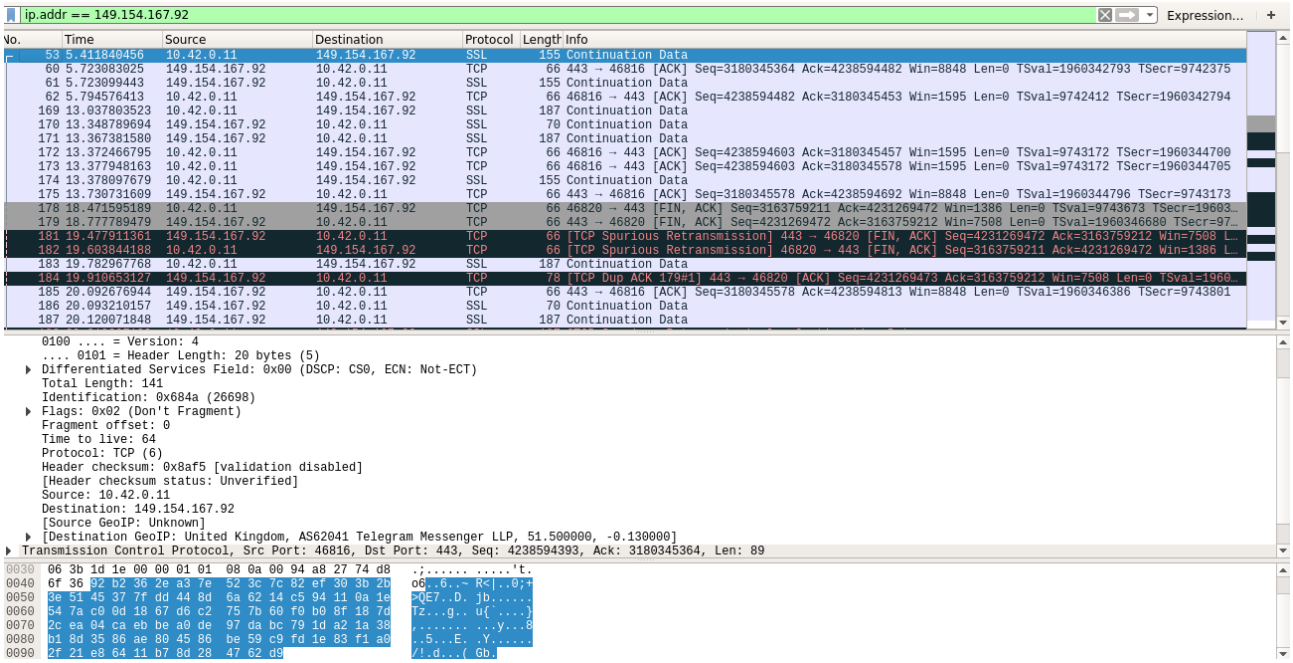
ابتدا عملیات برقراری ارتباط را انجام میدهد سپس با استفاده ازssl داده‌ها را میفرستد که در شکل زیر قابل مشاهده است

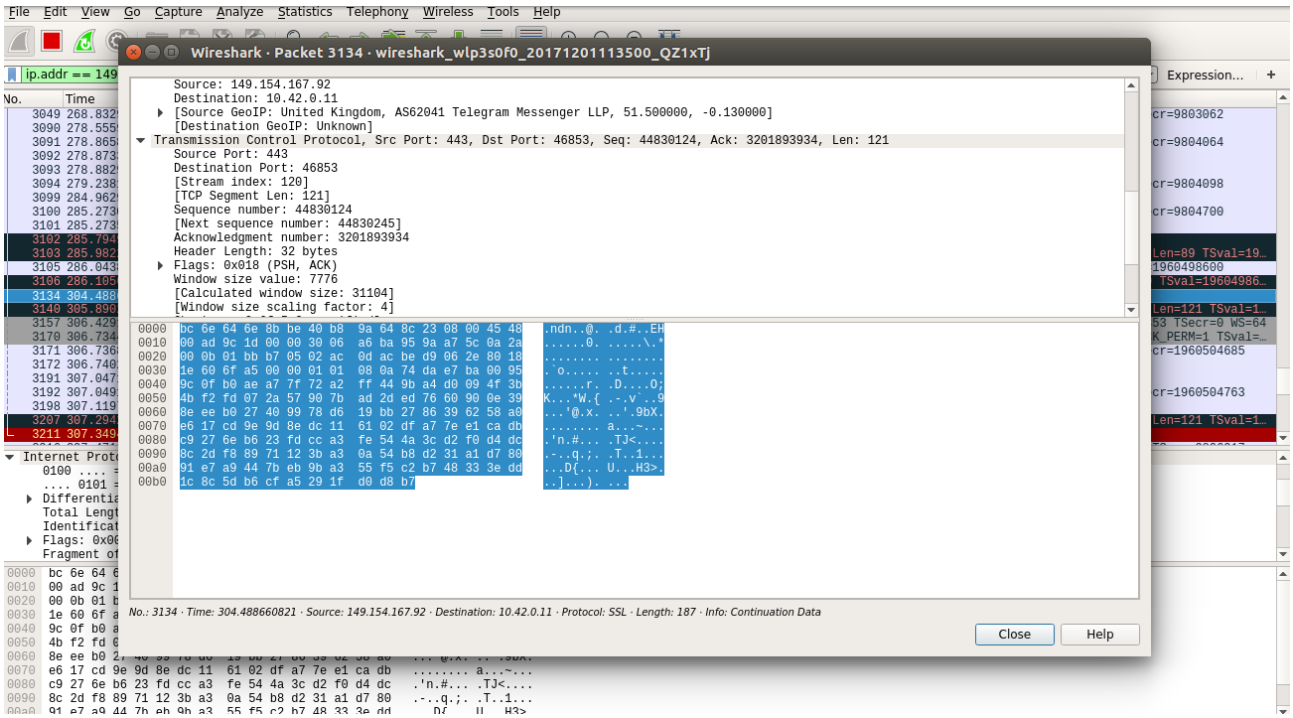


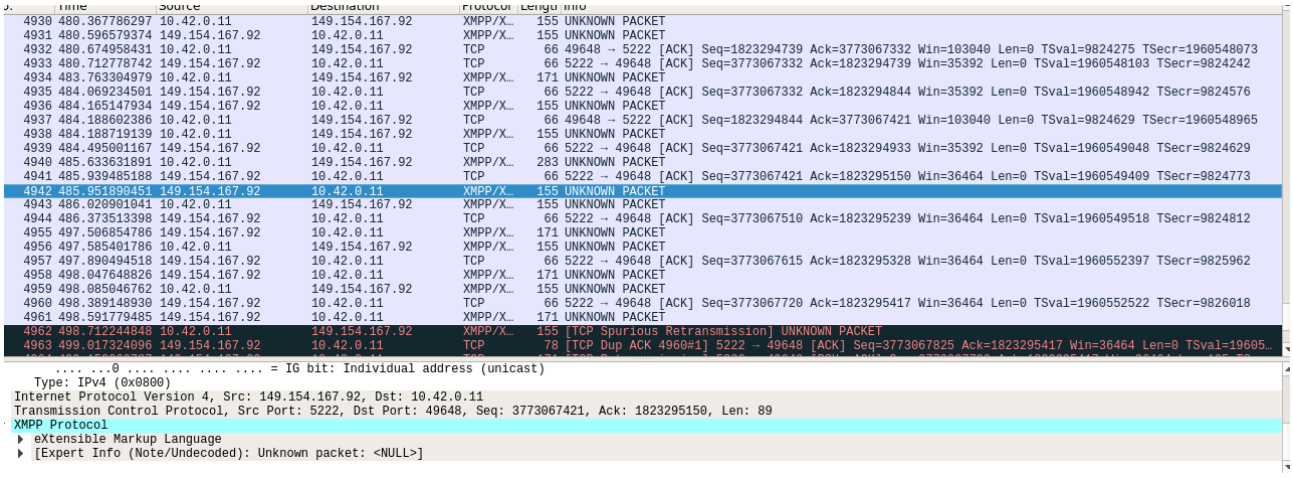


بخش سوم)

در حالت ابتدایی رمزنگاری وجود دارد ولی ضعیف‌تر از حالتsecret chat می‌باشد همچنین در حالتsecet chat به صورت انتها به انتها رمزگذاری انجام می‌شود


ip.addr == 149.154.167.92
Expression...
No. Time Source Destination Protocol Length Info
53 5.411840456 10.42.0.11 149.154.167.92 SSL 155 Continuation Data
60 5.723083025 149.154.167.92 10.42.0.11 TCP 66 443 → 46816 [ACK] Seq=3180345364 Ack=4238594482 Win=8848 Len=0 TSval=1960342793 TSecr=9742375
61 5.723099443 149.154.167.92 10.42.0.11 SSL 155 Continuation Data
62 5.794576413 10.42.0.11 149.154.167.92 TCP 66 46816 → 443 [ACK] Seq=4238594482 Ack=3180345453 Win=1595 Len=0 TSval=9742412 TSecr=1960342794
169 13.037803523 10.42.0.11 149.154.167.92 SSL 187 Continuation Data
170 13.348789694 149.154.167.92 10.42.0.11 SSL 70 Continuation Data
171 13.367381580 149.154.167.92 10.42.0.11 SSL 187 Continuation Data
172 13.372466795 10.42.0.11 149.154.167.92 TCP 66 46816 → 443 [ACK] Seq=4238594603 Ack=3180345457 Win=1595 Len=0 TSval=9743172 TSecr=1960344700
173 13.377948163 10.42.0.11 149.154.167.92 TCP 66 46816 → 443 [ACK] Seq=4238594603 Ack=3180345578 Win=1595 Len=0 TSval=9743172 TSecr=1960344705
174 13.378097679 10.42.0.11 149.154.167.92 SSL 155 Continuation Data
175 13.730731609 149.154.167.92 10.42.0.11 TCP 66 443 → 46816 [ACK] Seq=3180345578 Ack=4238594692 Win=8848 Len=0 TSval=1960344796 TSecr=9743173
178 18.471595189 10.42.0.11 149.154.167.92 TCP 66 46820 → 443 [FIN, ACK] Seq=3163759211 Ack=4231269472 Win=1386 Len=0 TSval=9743673 TSecr=19603…
179 18.777789479 149.154.167.92 10.42.0.11 TCP 66 443 → 46820 [FIN, ACK] Seq=4231269472 Ack=3163759212 Win=7508 Len=0 TSval=1960346680 TSecr=97…
181 19.477911361 149.154.167.92 10.42.0.11 TCP 66 [TCP Spurious Retransmission] 443 → 46820 [FIN, ACK] Seq=4231269472 Ack=3163759212 Win=7508 L…
182 19.603844188 10.42.0.11 149.154.167.92 TCP 66 [TCP Spurious Retransmission] 46820 → 443 [FIN, ACK] Seq=3163759211 Ack=4231269472 Win=1386 L…
183 19.782967768 10.42.0.11 149.154.167.92 SSL 187 Continuation Data
184 19.910653127 149.154.167.92 10.42.0.11 TCP 78 [TCP Dup ACK 179#1] 443 → 46820 [ACK] Seq=4231269473 Ack=3163759212 Win=7508 Len=0 TSval=1960…
185 20.092676944 149.154.167.92 10.42.0.11 TCP 66 443 → 46816 [ACK] Seq=3180345578 Ack=4238594813 Win=8848 Len=0 TSval=1960346386 TSecr=9743801
186 20.093210157 149.154.167.92 10.42.0.11 SSL 70 Continuation Data
187 20.120071848 149.154.167.92 10.42.0.11 SSL 187 Continuation Data
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 141
Identification: 0x684a (26698)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x8af5 [validation disabled]
[Header checksum status: Unverified]
Source: 10.42.0.11
Destination: 149.154.167.92
[Source GeoIP: Unknown]
[Destination GeoIP: United Kingdom, AS62041 Telegram Messenger LLP, 51.500000, -0.130000]
Transmission Control Protocol, Src Port: 46816, Dst Port: 443, Seq: 4238594393, Ack: 3180345364, Len: 89
0030 06 3b 1d 1e 00 00 01 01 08 0a 00 94 a8 27 74 d8 .;..... .....'t.
0040 6f 36 92 b2 36 2e a3 7e 52 3c 7c 82 ef 30 3b 2b o6..6..~ R<|..0;+
0050 3e 51 45 37 7f dd 44 8d 6a 62 14 c5 94 11 0a 1e >QE7..D. jb.....
0060 54 7a c0 0d 18 67 d6 c2 75 7b 60 f0 b0 8f 18 7d Tz...g.. u{`....}
0070 2c ea 04 ca eb be a0 de 97 da bc 79 1d a2 1a 38 ,..... ...y...8
0080 b1 8d 35 86 ae 80 45 86 be 59 c9 fd 1e 83 f1 a0 ..5...E. .Y.....
0090 2f 21 e8 64 11 b7 8d 28 47 62 d8 /!.d...(Gb.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 3134 · wireshark_wlp3s0f0_20171201113500_QZ1xTj
Source: 149.154.167.92
Destination: 10.42.0.11
[Source GeoIP: United Kingdom, AS62041 Telegram Messenger LLP, 51.500000, -0.130000]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 443, Dst Port: 46853, Seq: 44830124, Ack: 3201893934, Len: 121
Source Port: 443
Destination Port: 46853
[Stream index: 120]
[TCP Segment Len: 121]
Sequence number: 44830124
[Next sequence number: 44830245]
Acknowledgment number: 3201893934
Header Length: 32 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 7776
[Calculated window size: 31104]
[Window size scaling factor: 4]
0000 bc 6e 64 6e 8b be 40 b8 9a 64 8c 23 08 00 45 48 .ndn..@. .d.#..EH
0010 00 ad 9c 1d 00 00 30 06 a6 ba 95 9a a7 5c 0a 2a ......0. .....\.*
0020 00 0b 01 bb b7 05 02 ac 0d ac be d9 06 2e 80 18 ....
0030 1e 60 6f a5 00 00 01 01 08 0a 74 da e7 ba 00 95 .`o..... ..t.....
0040 9c 0f b0 ae a7 7f 72 a2 ff 44 9b a4 d0 09 4f 3b ......r. .D....O;
0050 4b f2 fd 07 2a 57 90 7b ad 2d ed 76 60 90 0e 39 K...*W.{ .-.v`..9
0060 8e ee b0 27 40 99 78 d6 19 bb 27 86 39 62 58 a0 ...'@.x. ..'.9bX.
0070 e6 17 cd 9e 9d 8e dc 11 61 02 df a7 7e e1 ca db .... a...~...
0080 c9 27 6e b6 23 fd cc a3 fe 54 4a 3c d2 f0 d4 dc .'n.#... .TJ<....
0090 8c 2d f8 89 71 12 3b a3 0a 54 b8 d2 31 a1 d7 80 .-..q.;. .T..1...
00a0 91 e7 a9 44 7b eb 9b a3 55 f5 c2 b7 48 33 3e dd ...D{... U...H3>.
00b0 1c 8c 5d b6 cf a5 29 1f d0 d8 b7 ..]...). ...
No.: 3134 · Time: 304.488660821 · Source: 149.154.167.92 · Destination: 10.42.0.11 · Protocol: SSL · Length: 187 · Info: Continuation Data
Close
Help



	Time	Source	Destination	Protocol	Length	Info
4930	480.367786297	10.42.0.11	149.154.167.92	XMPP/X…	155	UNKNOWN PACKET
4931	480.596579374	149.154.167.92	10.42.0.11	XMPP/X…	155	UNKNOWN PACKET
4932	480.674958431	10.42.0.11	149.154.167.92	TCP	66	49648 → 5222 [ACK] Seq=1823294739 Ack=3773067332 Win=103040 Len=0 TSval=9824275 TSecr=1960548073
4933	480.712778742	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067332 Ack=1823294739 Win=35392 Len=0 TSval=1960548103 TSecr=9824242
4934	483.763304979	10.42.0.11	149.154.167.92	XMPP/X…	171	UNKNOWN PACKET
4935	484.069234501	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067332 Ack=1823294844 Win=35392 Len=0 TSval=1960548942 TSecr=9824576
4936	484.165147934	149.154.167.92	10.42.0.11	XMPP/X…	155	UNKNOWN PACKET
4937	484.188602386	10.42.0.11	149.154.167.92	TCP	66	49648 → 5222 [ACK] Seq=1823294844 Ack=3773067421 Win=103040 Len=0 TSval=9824629 TSecr=1960548965
4938	484.188719139	10.42.0.11	149.154.167.92	XMPP/X…	155	UNKNOWN PACKET
4939	484.495001167	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067421 Ack=1823294933 Win=35392 Len=0 TSval=1960549048 TSecr=9824629
4940	485.633631891	10.42.0.11	149.154.167.92	XMPP/X…	283	UNKNOWN PACKET
4941	485.939485188	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067421 Ack=1823295150 Win=36464 Len=0 TSval=1960549409 TSecr=9824773
4942	485.951890451	149.154.167.92	10.42.0.11	XMPP/X…	155	UNKNOWN PACKET
4943	486.020901041	10.42.0.11	149.154.167.92	XMPP/X…	155	UNKNOWN PACKET
4944	486.373513398	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067510 Ack=1823295239 Win=36464 Len=0 TSval=1960549518 TSecr=9824812
4955	497.506854786	149.154.167.92	10.42.0.11	XMPP/X…	171	UNKNOWN PACKET
4956	497.585401786	10.42.0.11	149.154.167.92	XMPP/X…	155	UNKNOWN PACKET
4957	497.890494518	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067615 Ack=1823295328 Win=36464 Len=0 TSval=1960552397 TSecr=9825962
4958	498.047648826	149.154.167.92	10.42.0.11	XMPP/X…	171	UNKNOWN PACKET
4959	498.085046762	10.42.0.11	149.154.167.92	XMPP/X…	155	UNKNOWN PACKET
4960	498.389148930	149.154.167.92	10.42.0.11	TCP	66	5222 → 49648 [ACK] Seq=3773067720 Ack=1823295417 Win=36464 Len=0 TSval=1960552522 TSecr=9826018
4961	498.591779485	149.154.167.92	10.42.0.11	XMPP/X…	171	UNKNOWN PACKET
4962	498.712244848	10.42.0.11	149.154.167.92	XMPP/X…	155	[TCP Spurious Retransmission] UNKNOWN PACKET
4963	499.017324096	149.154.167.92	10.42.0.11	TCP	78	[TCP Dup ACK 4960#1] 5222 → 49648 [ACK] Seq=3773067825 Ack=1823295417 Win=36464 Len=0 TSval=19605…

```
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 149.154.167.92, Dst: 10.42.0.11
Transmission Control Protocol, Src Port: 5222, Dst Port: 49648, Seq: 3773067421, Ack: 1823295150, Len: 89
XMPP Protocol
▸ eXtensible Markup Language
▸ [Expert Info (Note/Undecoded): Unknown packet: <NULL>]
```

سؤال سوم

استفاده از ابزارهای مانیتورینگ به‌خصوص در سازمان هایی که ترافیک های یک کشور را بررسی میکنند بسیار مهم است. مثلاً ممکن است بدافزاری که اقدام به باج گیری میکند هنوز یک کشور خاص را آلوده نکرده اگر بتواند درگاه ها را تحلیل ترافیک کرد بسته های آلوده به این بدافزار ها را میتوان شناسایی نمود و جلوی گسترش بیش از اندازه آن را گرفت.

یا مثلاً فرض کنید یک کشور که دارای چندین درگاه برای ورود ترافیک میباشد و الگوری های منظمی از این ترافیک دارد ناگهان به این موضوع برخورد میکند که از یک درگاه ترافیک بیش از اندازه وارد کشور شده است همین میتواند مسوولان را نسبت به این موضوع حساس کند که احتمالاً حمله ای در حال رخ دادن است..

از طرفی در تصمیم گیری های کلان یک کشور میتوان با تحلیل ترافیک و مشخص نمود الگوی تمایل مردم به محتواهای مختلف ، سلیقه مردم یک کشور را مشخص نمود مثلاً تصور کنید کشوری که بیشترین ترافیک داخلی آن مربوط به سایت‌های خبری باشد بعد از چند سال ترافیک اصلی آن بر روی سرور های سایت‌های سرگرمی قرار میگیرد این به منزله تغییر ذایقه مردم می باشد.