# به نام خدا

# محمدمهدی آقاجانی

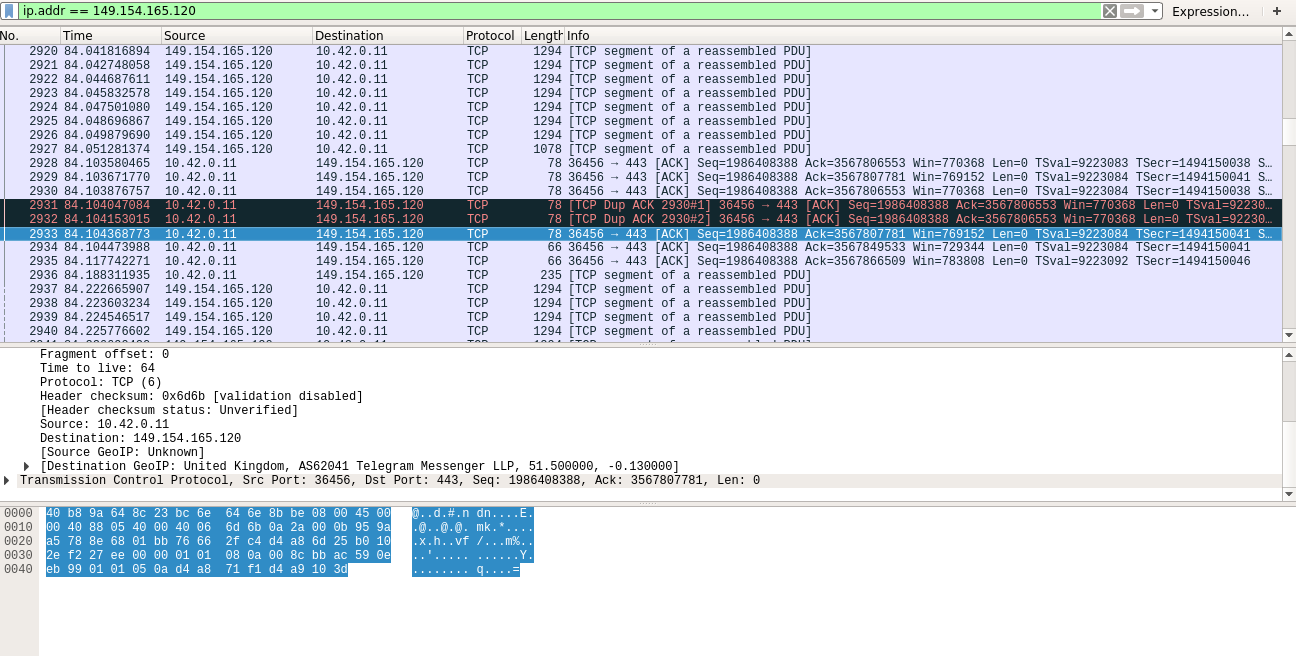
# 9331056

# تمرین عملی اول

# استاد : دکتر شهریاری

سؤال اول

پروتکل های مورد استفاده بیشترssl , 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 )

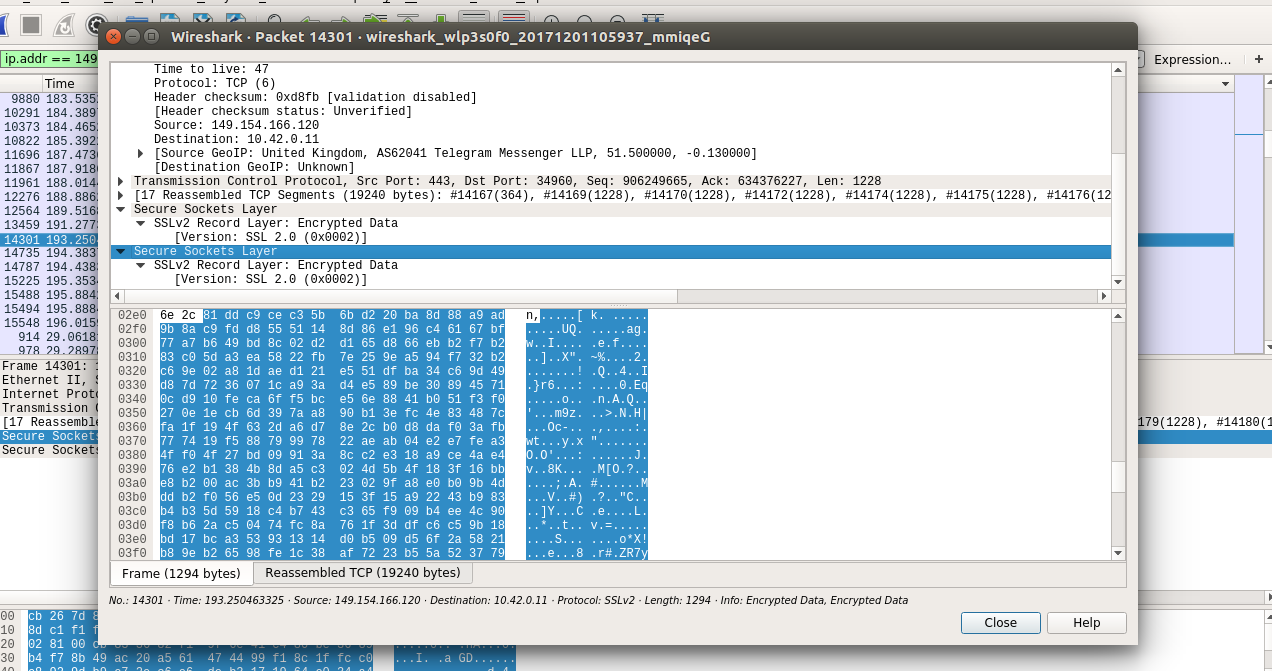
91.108.4.134

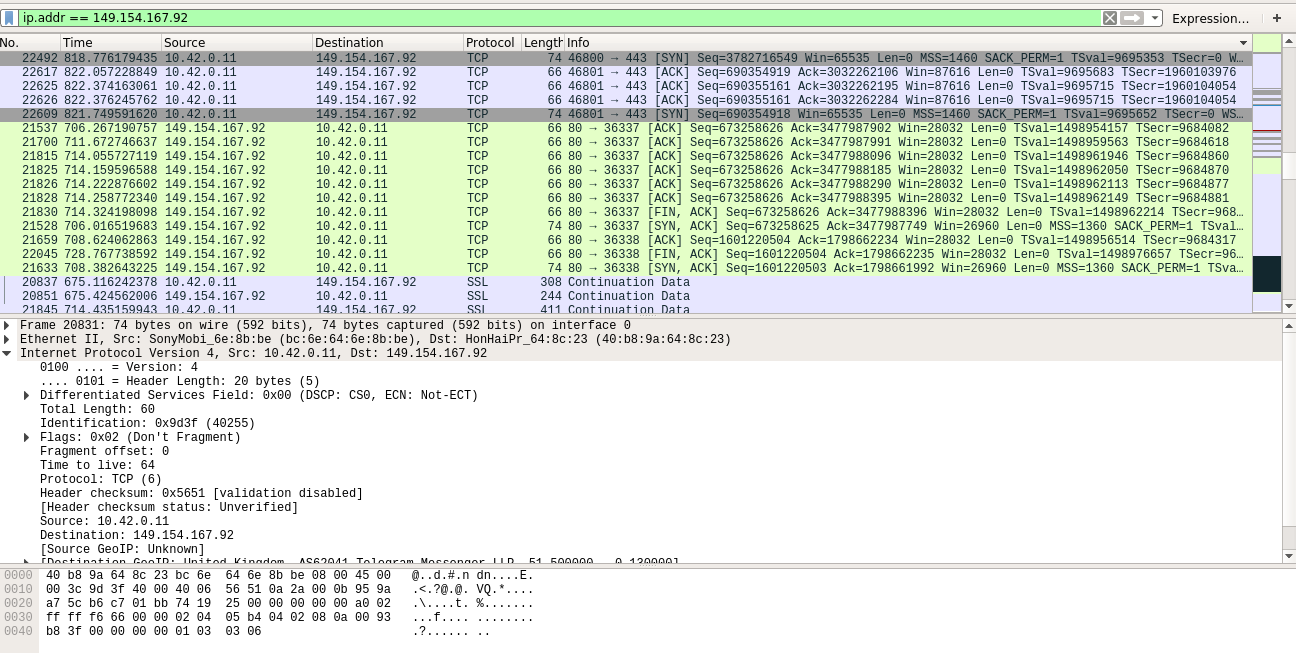
149.154.166.120

149.154.167.92

بخش دوم )

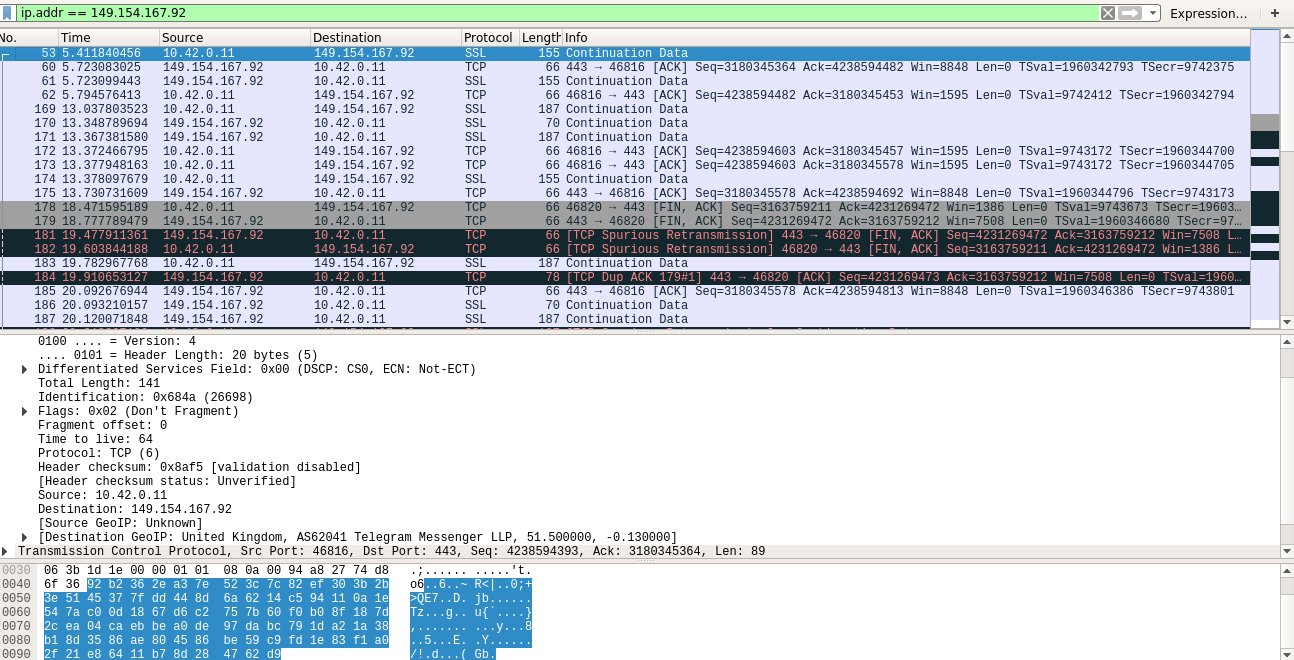
ابتدا عملیات برقراری ارتباط را انجام میدهد سپس با استفاده ازssl داده‌ها را میفرستد که در شکل زیر قابل مشاهده است

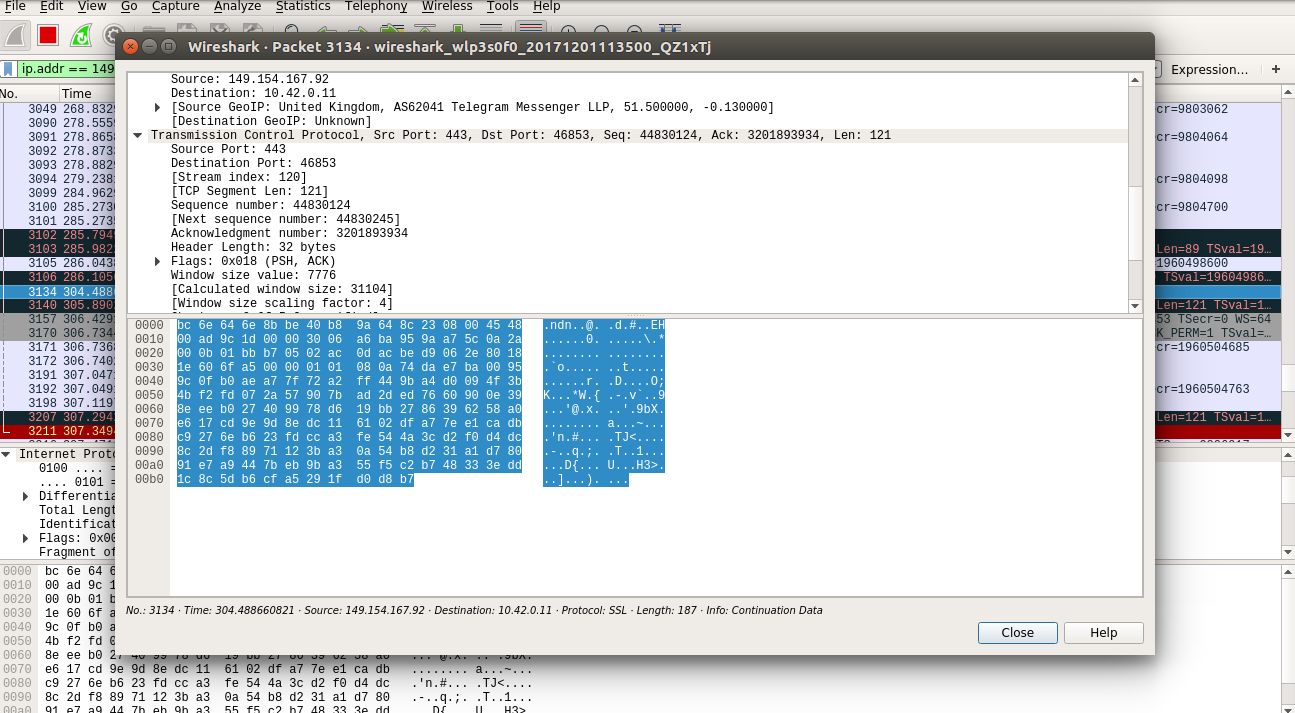


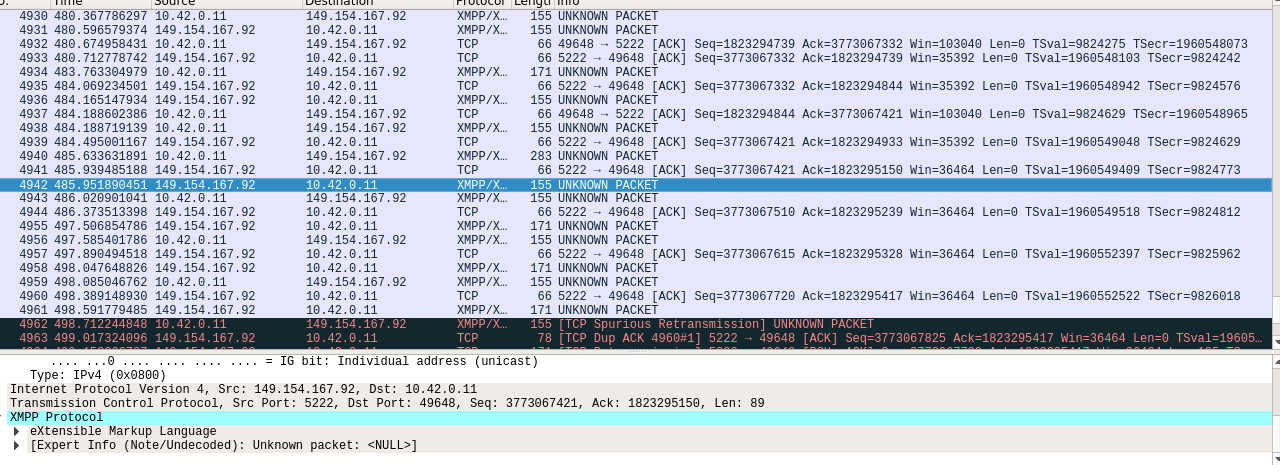


بخش سوم )

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







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.