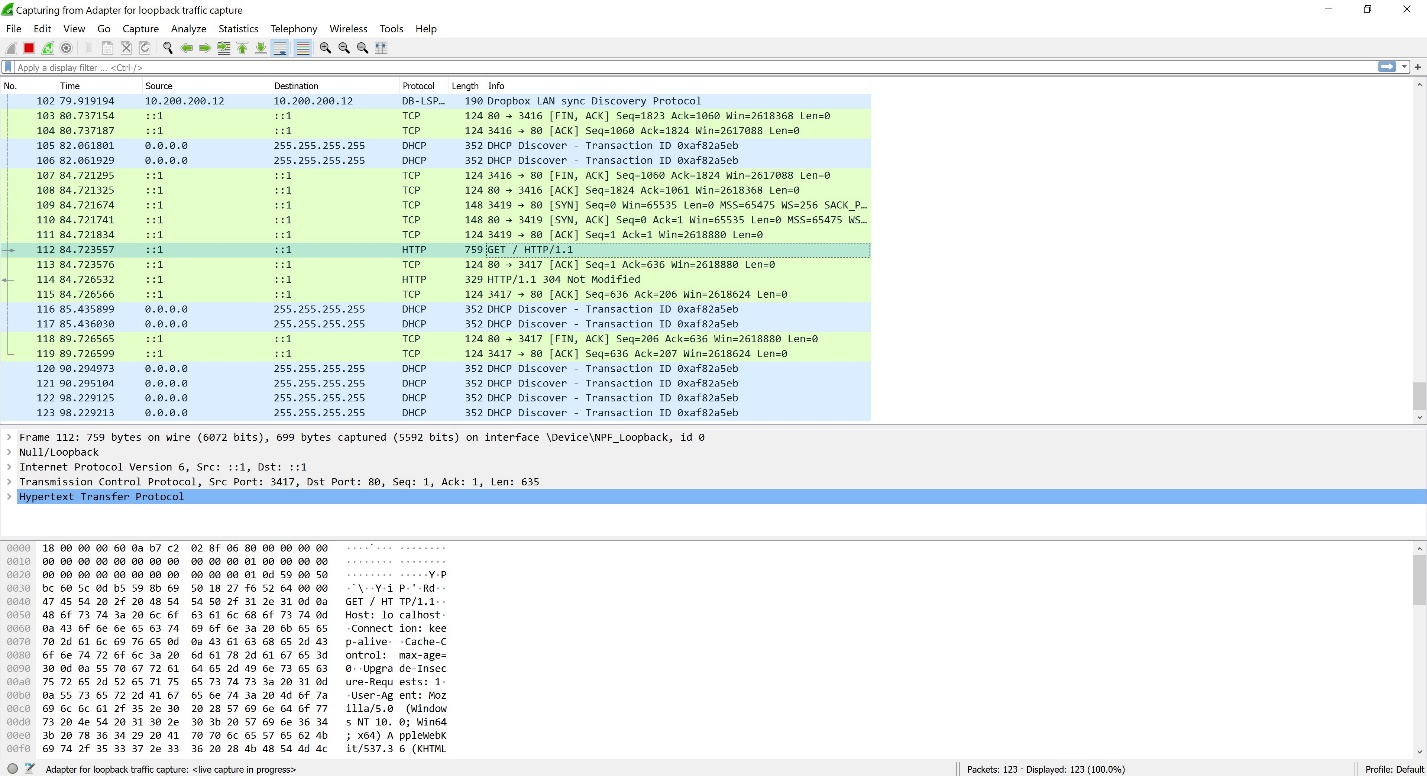
علی نظری – ۹۶۳۱۰۷۵

آزمایشگاه شبکه – سه‌شنبه‌ها ساعت ۱۶:۳۰

آزمایش مربوط به ۴ شهریور ۹۹

چون در حقیقت ما مشخص نکردیم که این دامنه متناظر با چه آدرس ip ای است و تا وقتی که این موضوع را در فایل hosts مشخص نکردیم نمی‌توانیم به محتوای خود از طریق این دامنه دسترسی داشته باشیم.

همانطور که در شکل زیر و با کمک شبکه loopback مشخص شده، بسته ای که درخواست GET را از طریق پروتکل HTTP فرستاده است مطلوب مسئله ما است و همچنین در پایین تر می‌بینیم که که درخواست از چه پورت مبدایی به چه پورت مقصدی در localhost ارسال شده است.

پورت مبدا در این ارتباط به صورت تصادفی ۳۴۱۷ و پورت مقصد ۸۰ است.

ارتباط در این پروتکل به این صورت است که در ابتدا یک اتصال TCP برقرار می‌شود و سپس درخواست با روش‌های مختلف و همراه با اطلاعات مورد نیاز در قالب header, body ارسال می‌شود و پاسخ را دریافت می‌کند.

با کمک فایل hosts، ip متناظر این سایت را دریافت می‌کند و در غیر این صورت نیز باید با کمک سرویس DNS آدرس را پیدا کند.

مقدار این بخش keep-alive است به معنی اینکه این ارتباط برقرار بماند.

درخواست از نوع GET بوده است.

مقدار User Agent برابر است با:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36

که اطلاعاتی درباره سیستم عامل و مرورگر را همراه با این درخواست ارسال می‌کند.

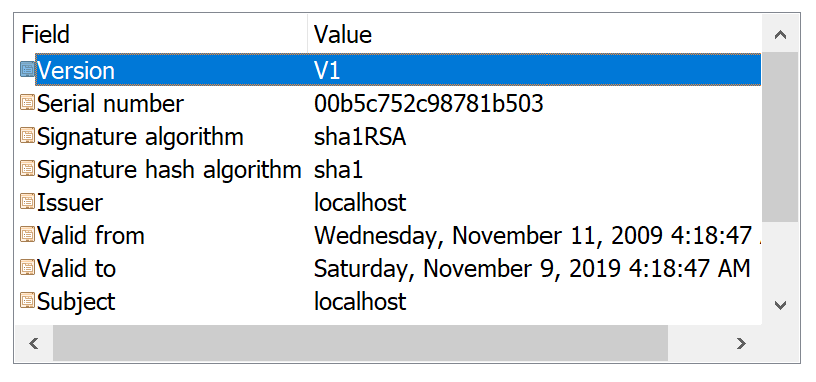
اگر اولین بسته را همان بسته‌ای که درخواست GET را ارسال کرده در نظر بگیریم، همه flagها صفر هستند به جز push و ack که یک هستند.

فقط هدر host در این دو با هم تفاوت دارد.

این درخواست مشکل دارد زیرا ما چند دامنه را نظیر با این ip کرده ایم و مشخص نیست درخواست ما کدام است.

با پیغام connection is not private رو به رو می‌شویم که به خاطر نامعتبر بودن SSL ای است که استفاده کرده ایم.

این گواهی توسط localhost برای localhost ساخته شده بود.

اعتبار این گواهی سال ۲۰۱۹ به پایان رسیده بود. اطلاعات کلید عمومی و امضای آن هم در تصویر زیر قابل مشاهده است.

این ارتباط قابل خواندن نیست زیرا رمز گذاری شده است و فقط با استفاده از کلید خصوصی آن می‌توان آن را فهمید.

با توجه به اینکه این سایت از گواهی معتبری استفاده می‌کند، مرورگر ما با خطا رو به رو نمی‌شود.

سازنده این گواهی و مدت اعتبار آن که برای گوگل ساخته شده است با ما فرق می‌کند.

همچنین الگوریتم‌های رمز نگاری این گواهی نیز با آن چیزی که ما داشتیم تفاوت دارد.

برای لیست کردن فایل‌ها از دستور LIST -l استفاده شده است.

نام کاربری استفاده شده برای دسترسی ali است که قبلا در filezilla admin تنظیم شده بود.

پروتکل لایه انتقال که استفاده شده TCP است.

پورت مبدا برابر ۶۰۳۳ است و پورت مقصد که پورت پیش‌فرض برای پروتکل ftp است برابر ۲۱ می‌باشد.

بله دستور PASS 123456 مشاهده می‌شود که همان پسورد ali است و در جواب هم پاسخ درست Logged on دریافت شده است.

برای کاربر ali دسترسی‌ای با مشخصات read و list بر روی دایرکتوری C:\Users\Ali\Downloads\Telegram Desktop تنظیم شده است.

سوال ۱۵ و ۱۶ هم حذف شد.