آزمایش شماره ۳

آز شبکه - دکتر بردیا صفایی

دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف

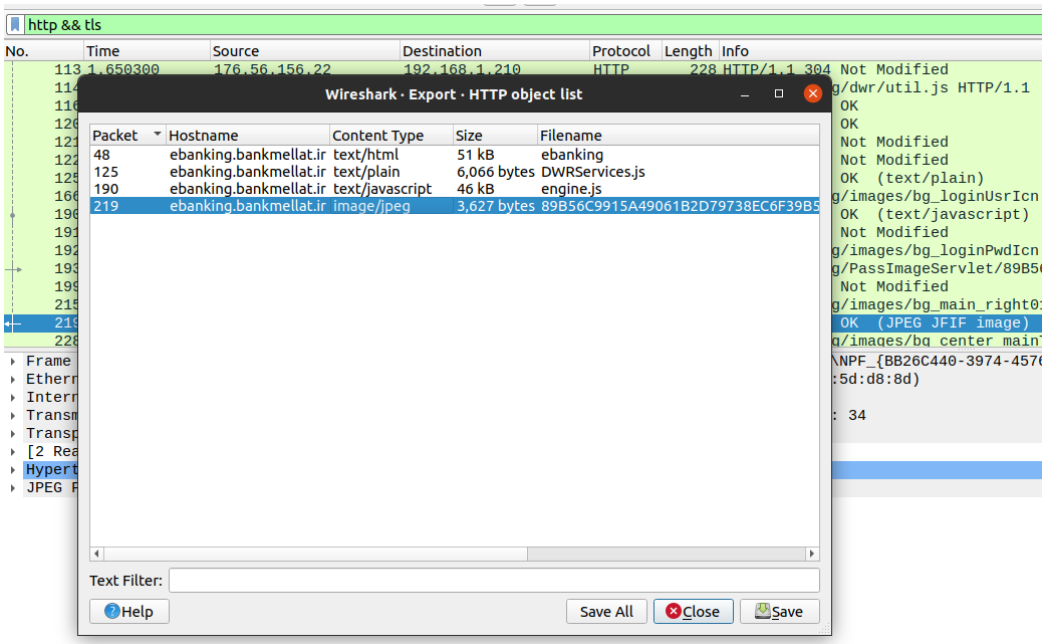
نیم‌سال اول ۰۱-۰۲

مهرشاد میرمحمدی - ۹۸۱۰۹۶۳۴
پرهام صارمی - ۹۷۱۰۱۹۵۹
محمدرضا مفیضی - ۹۸۱۰۶۰۵۹

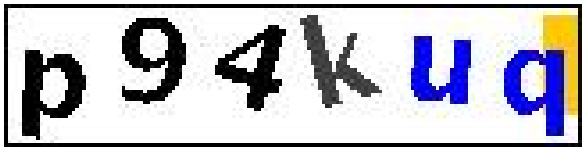
۱ wireshark

۱.۱ بدست‌آوردن captcha

همانند دستور عمل می‌کنیم، با این تفاوت که به جای استفاده ازهمانند دستور عمل می‌کنیم، با این تفاوت که به جای استفاده از SSL ، از TLS استفاده می‌کنیم. دلیل آن هم این است که SSL منسوخ شده و TLS جای آن را گرفته است. همچنین این پروتکل در ورژن wireshark مورد استفاده موجود نبود. لیست فایل‌های استخراج شده و یcaptcha بدست‌آمده را می‌توان در تصاویر ۱ و ۲ دید.



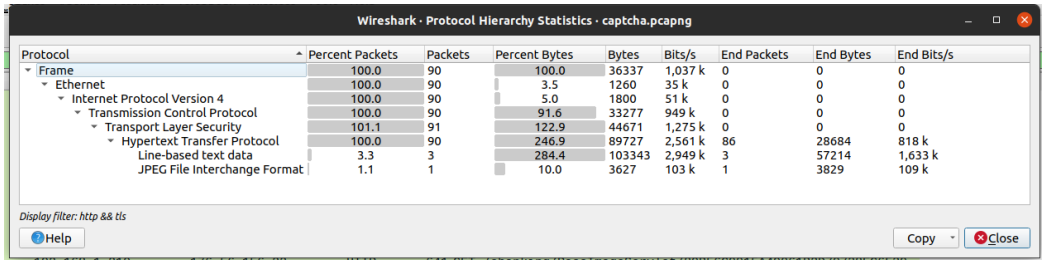
شکل ۱ : پنجره‌ی ذخیره‌سازی فایل‌های بدست‌آمده.



شکل ۲ : عکس بدست‌آمده.

۲.۱ سوال‌ها

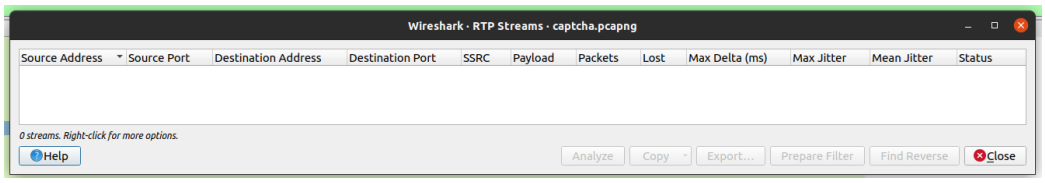
۱. این اطلاعات و آماره‌ها را می‌توان از طریق منوی statistics موجود در wireshark بدست آورد. برای مثال با استفاده از بخش سلسله مراتب پروتکل‌ها می‌توان دید پروتکل‌های استفاده شده کدام‌ها هستند، از هر کدام چند پکت موجود است و چند درصد از پکت‌ها و بایت‌ها برای آن بوده است. تصویر ۳ نمونه خروجی این ابزار است. همچنین با استفاده از باقی ابزارها می‌توان اطلاعات دیگری همانند طول بسته‌ها، ترافیک و تعداد بسته‌های بین بخش‌های مختلف شبکه، زمان بین پاسخ‌ها و ... بدست‌آورد.



شکل ۳: Hierarchy Protocols < statistics

۲. پروتکل RTP یک پروتکل بیدرنگ برای انتقال صدا و تصویر در شبکه‌ها با بستر IP است. این پروتکل معمولا بر پایه‌ی UDP است و برای streaming استفاده می‌شود. همچنین معمولا برای کنترل ترتیب رسیدن بسته‌ها، از پرتوکل RTCP هم به همراه آن استفاده می‌شود.

در wireshark می‌توان با رفتن به Telephony سپس RTP و سپس streams RTP اطلاعات مربوط به آن را یافت. اطلاعاتی مانند آدرس و پورت مبدا و مقصد، میانگین و حداکثر jitter ، گمشدگی و ... که در تصویر ۴ هم می‌توان دید. همچنین امکان ضبط و بخش محتوا به صورت مستقیم هم موجود است.



شکل ۴: Streams RTP < RTP < Telephony