



## آزمایش شماره ۳

آز شبکه - دکتر بردیا صفایی

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

نیم سال اول ۰۱-۰۲

مهرشاد میرمحمدی - ۹۸۱۰۹۶۳۴

پرهام صارمی - ۹۷۱۰۱۹۵۹

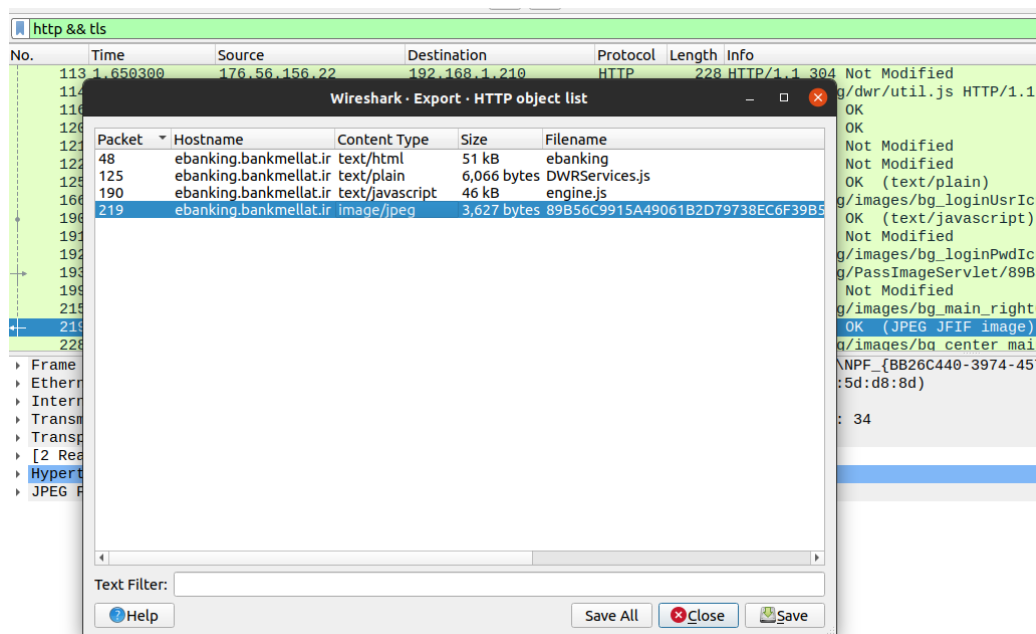
محمدرضا مفیضی - ۹۸۱۰۶۰۵۹



## ۱ wireshark

## ۱.۱ بدست آوردن captcha

همانند دستور عمل می‌کنیم، با این تفاوت که به جای استفاده از همانند 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 ی captcha بدست آمده را می‌توان در تصاویر ۱ و ۲ دید.



شکل ۱: پنجره‌ی ذخیره‌سازی فایل‌های بدست آمده.



شکل ۲: عکس بدست آمده.

## ۲.۱ سوال‌ها

۱. این اطلاعات و آمارها 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 ... بدست آورد.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	90	100.0	36337	1,037 k	0	0	0
Ethernet	100.0	90	3.5	1260	35 k	0	0	0
Internet Protocol Version 4	100.0	90	5.0	1800	51 k	0	0	0
Transmission Control Protocol	100.0	90	91.6	33277	949 k	0	0	0
Transport Layer Security	101.1	91	122.9	44671	1,275 k	0	0	0
Hypertext Transfer Protocol	100.0	90	246.9	89727	2,561 k	86	28684	818 k
Line-based text data	3.3	3	284.4	103343	2,949 k	3	57214	1,633 k
JPEG File Interchange Format	1.1	1	10.0	3627	103 k	1	3829	109 k

Display filter: http && tls

Help Copy Close

شکل ۳: Hierarchy Protocols &lt; statistics

۲. پروتکل RTP یک پروتکل بیدرنگ برای انتقال صدا و تصویر در شبکه‌ها با بستر IP است. این پروتکل معمولاً بر پایه‌ی UDP است و برای streaming استفاده می‌شود. همچنین معمولاً برای کنترل ترتیب رسیدن بسته‌ها، از پروتکل 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.

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
0 streams. Right-click for more options.											

Help Analyze Copy Export... Prepare Filter Find Reverse Close

شکل ۴: Streams RTP &lt; RTP &lt; Telephony