آز شبکه

نیم‌سال اول ۰۱-۰۲

مدرس: دکتر صفائی

دانشکده مهندسی کامپیوتر

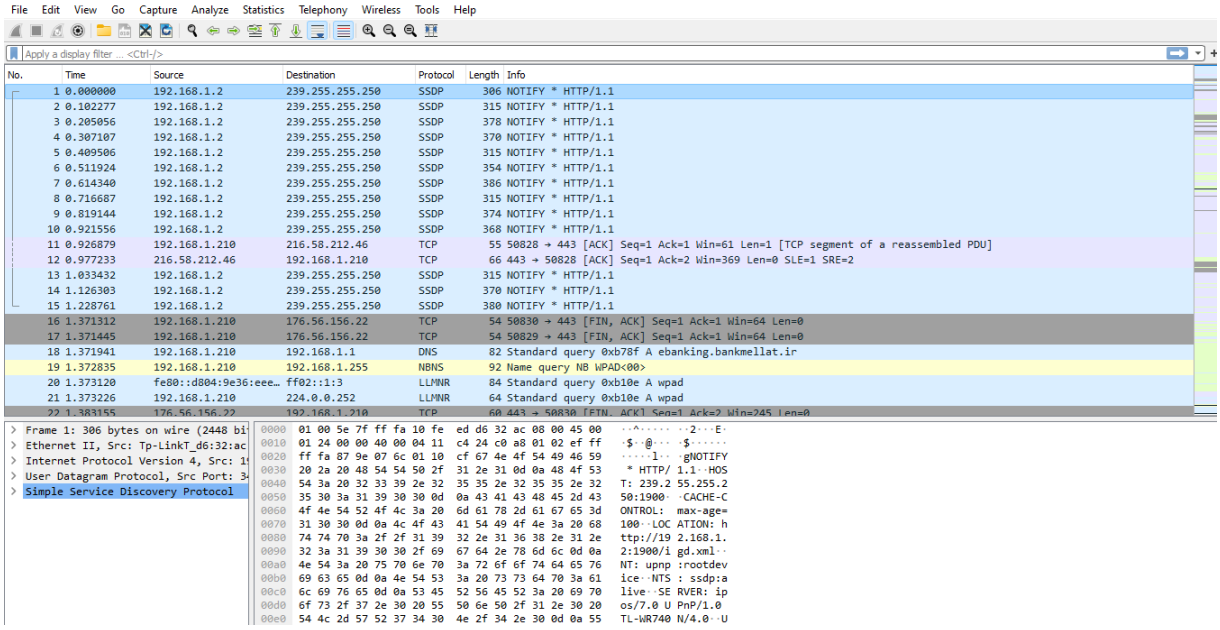
آزمایش سوم

پارسا رئیسی : ۹۸۱۰۳۲۲۳ عماد زین‌اوقلی : ۹۸۱۰۳۲۶۷ سیدابوالفضل رحیمی : ۹۷۱۰۵۹۴۱

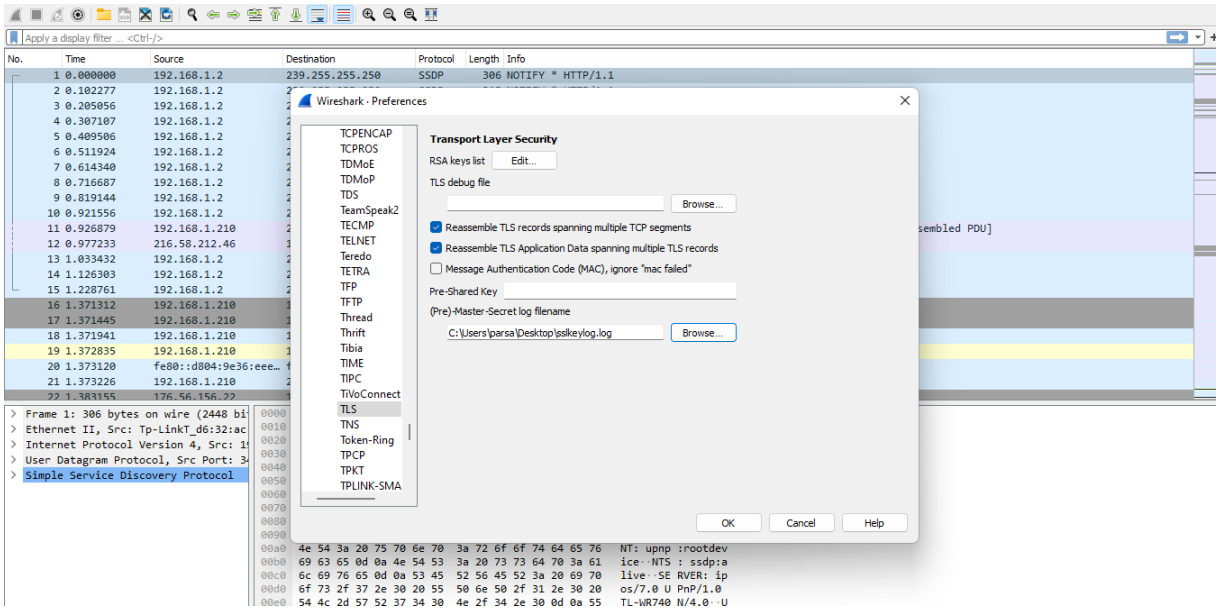
۱- Wireshark

۱.۱ بدست آوردن captcha

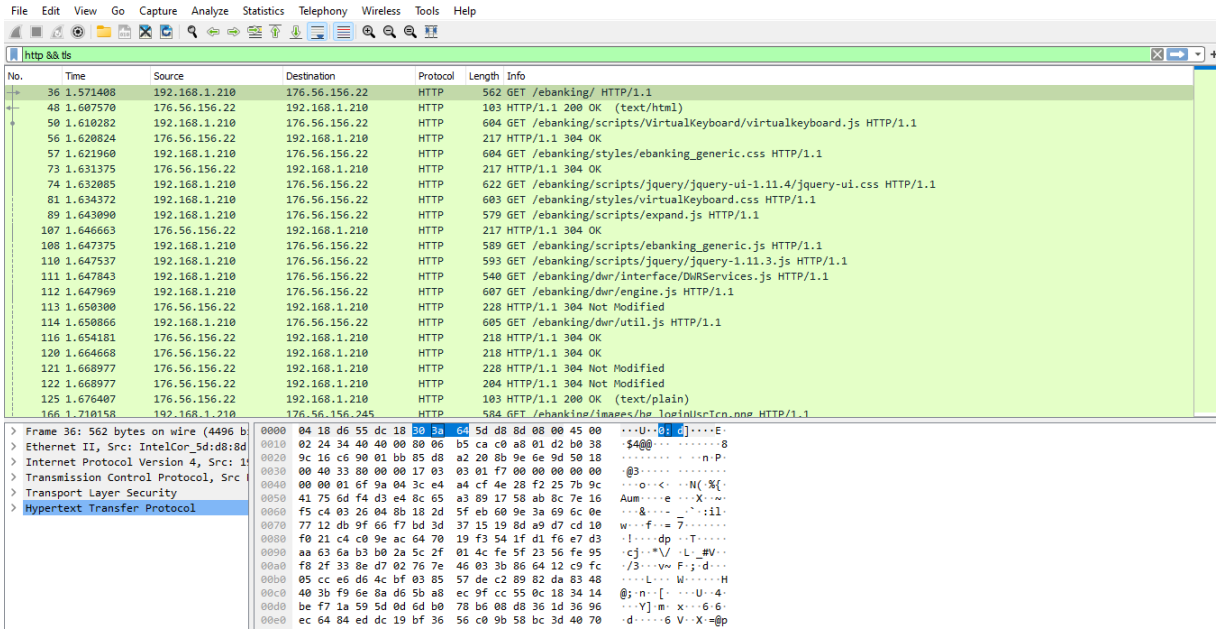
فایل را در نرم‌افزار باز می‌کنیم.



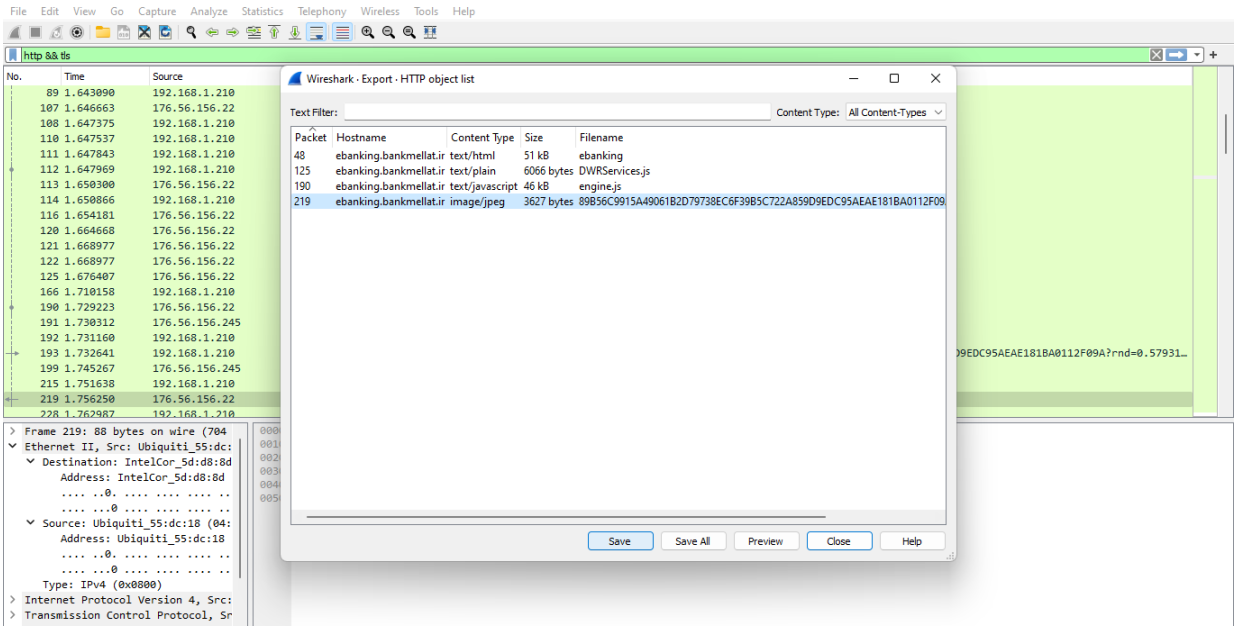
فایل sslkeylog را در قسمت خواسته‌شده آپلود می‌کنیم.



فیلتر ها را اعمال می‌کنیم.



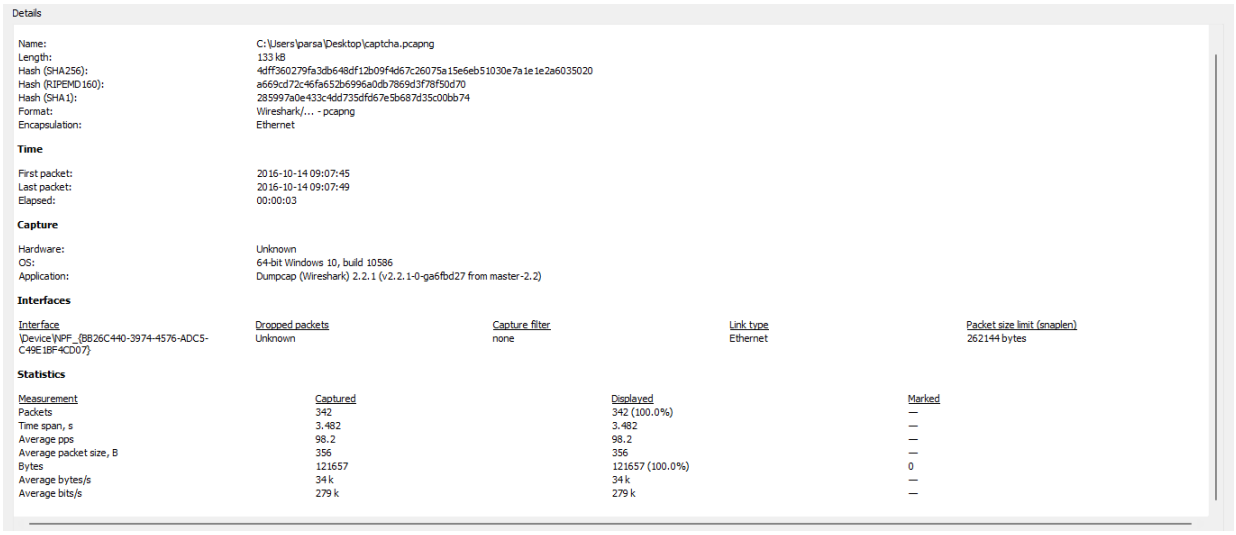
فایل تصویر captcha را ذخیره می‌کنیم.



تصویر captcha :

۲.۱ سوال‌ها

۱. آماره های مربوط به capture انجام‌شده را می‌توان در قسمت capture file properties مطابق تصویر زیر مشاهده کرد.



Details

Name:	C:\Users\parsa\Desktop\captcha.pcapng
Length:	133 kB
Hash (SHA256):	4dff360279fa3db648df12b09f4d67c26075a15e6eb51030e7a1e1e2a6035020
Hash (RIPEMD160):	a669cd72c46fa652b6996a0db7869d3f78f50d70
Hash (SHA1):	285997a0e433c4dd735dfd67e5b687d35c00bb74
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2016-10-14 09:07:45
Last packet:	2016-10-14 09:07:49
Elapsed:	00:00:03

Capture

Hardware:	Unknown
OS:	64-bit Windows 10, build 10586
Application:	Dumpcap (Wireshark) 2.2.1 (v2.2.1-0-ga6fbd27 from master-2.2)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
\Device\NPF_{BB26C440-3974-4576-ADC5-C49E1BF4CD07}	Unknown	none	Ethernet	262144 bytes

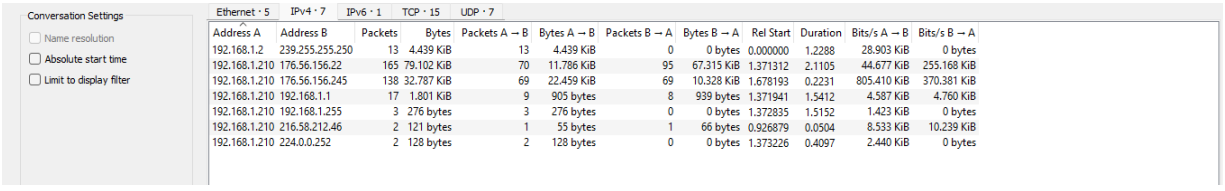
Statistics

Measurement	Captured	Displayed	Marked
Packets	342	342 (100.0%)	—
Time span, s	3.482	3.482	—
Average pps	98.2	98.2	—
Average packet size, B	356	356	—
Bytes	121657	121657 (100.0%)	0
Average bytes/s	34 k	34 k	—
Average bits/s	279 k	279 k	—

با استفاده از این فایل می‌توان تعداد بسته های ارسال شده، مدت زمان ضبط بسته ها، نرخ ارسال بسته ها و سایز متوسط بسته ها را مشاهده کرد. بنابراین اگر در یک مدت مشخص به نسبت کاری که انجام می‌دهیم، تعداد نامعمولی از بسته ها را ضبط کرده باشیم یا ناگهان بسته هایی با سایز غیرمعمول ضبط کنیم، می‌توان متوجه یک فعالیت غیرمعمول روی host شویم. و درصورت مشاهده چنین فعالیت غیرمعمولی، دقیق تر بسته های دریافتی و ارسالی را بررسی کنیم.

همچنین می‌توان از قسمت conversations بر اساس لایه های مختلف آدرس، اطلاعاتی درباره conversation های در هر لایه بدست آورد. با داشتن این دست اطلاعات مانند تعداد conversation ها در هر لایه، زمان نسبی شروع هر conversation ، مدت زمانی که هر conversation طول کشیده و طرف های هر conversation ، و با درنظر داشتن کاری که درحال انجام آن بودیم، می‌توانیم اطلاعاتی درباره رفتار شبکه و endpoint ها بدست آوریم. برای مثال دانستن این رفتار ها،در عیب‌یابی و تشخیص حمله و ... می‌تواند کمک‌کننده باشد.

در ادامه نمونه هایی از لایه شبکه و انتقال فایل موردنظر آورده شده‌است.



Conversation Settings

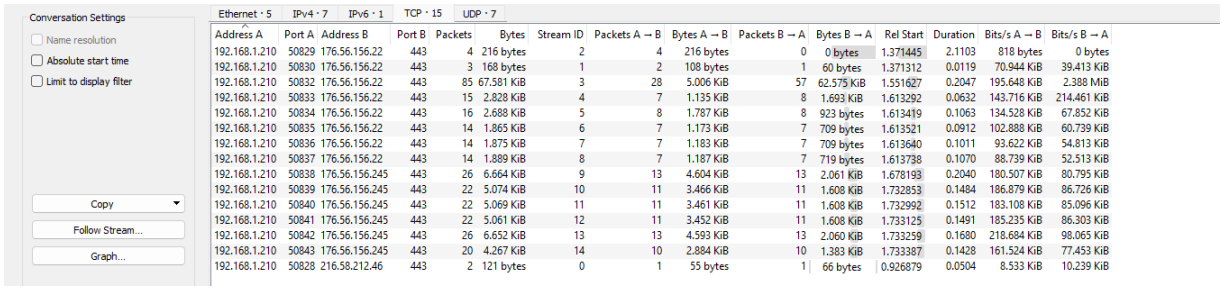
Name resolution

Absolute start time

Limit to display filter

Ethernet · 5 | IPv4 · 7 | IPv6 · 1 | TCP · 15 | UDP · 7

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.2	239.255.255.250	13	4.439 KiB	13	4.439 KiB	0	0 bytes	0.000000	1.2288	28.903 KiB	0 bytes
192.168.1.210	176.56.156.22	165	79.102 KiB	70	11.786 KiB	95	67.315 KiB	1.371312	2.1105	44.677 KiB	255.168 KiB
192.168.1.210	176.56.156.245	138	32.787 KiB	69	22.459 KiB	69	10.328 KiB	1.678193	0.2231	805.410 KiB	370.381 KiB
192.168.1.210	192.168.1.1	17	1.801 KiB	9	905 bytes	8	939 bytes	1.371941	1.5412	4.587 KiB	4.760 KiB
192.168.1.210	192.168.1.255	3	276 bytes	3	276 bytes	0	0 bytes	1.372835	1.5152	1.423 KiB	0 bytes
192.168.1.210	216.58.212.46	2	121 bytes	1	55 bytes	1	66 bytes	0.926879	0.0504	8.533 KiB	10.239 KiB
192.168.1.210	224.0.0.252	2	128 bytes	2	128 bytes	0	0 bytes	1.373226	0.4097	2.440 KiB	0 bytes



Conversation Settings

Name resolution

Absolute start time

Limit to display filter

Copy

Follow Stream...

Graph...

Ethernet · 5 | IPv4 · 7 | IPv6 · 1 | TCP · 15 | UDP · 7

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.210	50829	176.56.156.22	443	4	216 bytes	2	4	216 bytes	0	0 bytes	1.371445	2.1103	818 bytes	0 bytes
192.168.1.210	50830	176.56.156.22	443	3	168 bytes	1	2	108 bytes	1	60 bytes	1.371312	0.0119	70.944 KiB	39.413 KiB
192.168.1.210	50832	176.56.156.22	443	85	67.581 KiB	3	28	5.006 KiB	57	62.575 KiB	1.551627	0.2047	195.648 KiB	2.388 MiB
192.168.1.210	50833	176.56.156.22	443	15	2.828 KiB	4	7	1.135 KiB	8	1.693 KiB	1.613292	0.0632	143.716 KiB	214.461 KiB
192.168.1.210	50834	176.56.156.22	443	16	2.688 KiB	5	8	1.787 KiB	8	923 bytes	1.613419	0.1063	134.528 KiB	67.852 KiB
192.168.1.210	50835	176.56.156.22	443	14	1.865 KiB	6	7	1.173 KiB	7	709 bytes	1.613521	0.0912	102.888 KiB	60.739 KiB
192.168.1.210	50836	176.56.156.22	443	14	1.875 KiB	7	7	1.183 KiB	7	709 bytes	1.613640	0.1011	93.622 KiB	54.813 KiB
192.168.1.210	50837	176.56.156.22	443	14	1.889 KiB	8	7	1.187 KiB	7	719 bytes	1.613738	0.1070	88.739 KiB	52.513 KiB
192.168.1.210	50838	176.56.156.245	443	26	6.664 KiB	9	13	4.604 KiB	13	2.061 KiB	1.678193	0.2040	180.507 KiB	80.795 KiB
192.168.1.210	50839	176.56.156.245	443	22	5.074 KiB	10	11	3.466 KiB	11	1.608 KiB	1.732853	0.1484	186.879 KiB	86.726 KiB
192.168.1.210	50840	176.56.156.245	443	22	5.069 KiB	11	11	3.461 KiB	11	1.608 KiB	1.732992	0.1512	183.108 KiB	85.096 KiB
192.168.1.210	50841	176.56.156.245	443	22	5.061 KiB	12	11	3.452 KiB	11	1.608 KiB	1.733125	0.1491	185.235 KiB	86.303 KiB
192.168.1.210	50842	176.56.156.245	443	26	6.652 KiB	13	13	4.593 KiB	13	2.060 KiB	1.733259	0.1680	218.684 KiB	98.065 KiB
192.168.1.210	50843	176.56.156.245	443	20	4.267 KiB	14	10	2.884 KiB	10	1.383 KiB	1.733387	0.1428	161.524 KiB	77.453 KiB
192.168.1.210	50828	216.58.212.46	443	2	121 bytes	0	1	55 bytes	1	66 bytes	0.926879	0.0504	8.533 KiB	10.239 KiB

۲. Real-time Transport Protocol یک پروتکل لایه انتقال است، که برای انتقال فایل های صوتی و تصویری استفاده می‌شود. این پروتکل روی پروتکل UDP اجرا می‌شود و برخی خواص پروتکل TCP را به پروتکل UDP اضافه می‌کند. به طوری که علاوه بر سرعت در انتقال فایل های صوتی و تصویری، به دلیل اضافه شدن فیلد های sequence number و timestamp، دقت و ترتیب ارسال ها را نیز خواهیم داشت. بنابراین از RTP در سیستم های شامل streaming media مانند اپلیکیشن های telephony و video teleconference استفاده می‌شود.

در نرم‌افزار wireshark از طریق منو telephony»RTP»RTPStreams داده های مربوط به بسته های RTP را بررسی کرد و اطلاعاتی مانند آدرس IP و پورت های مبدا و مقصد و درصد دیتای گم شده و ... را مشاهده کرد.