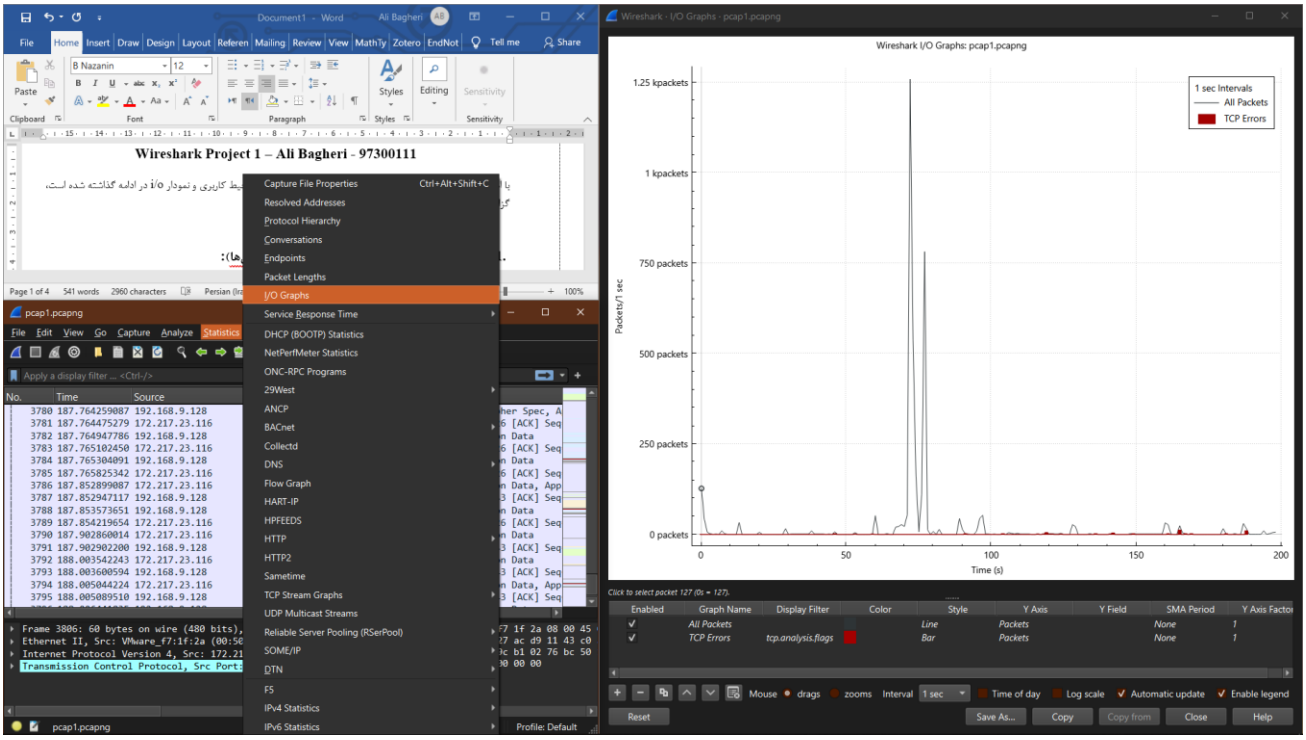
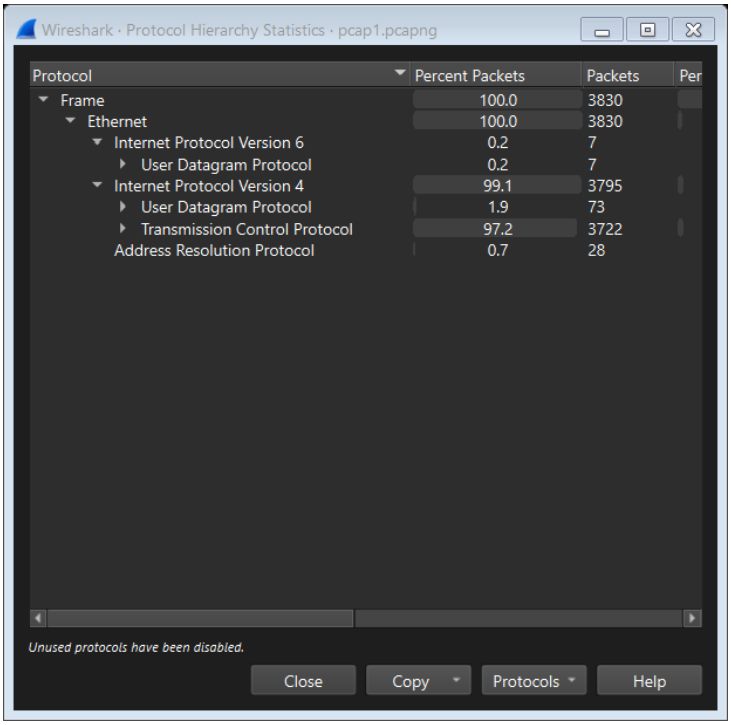
Wireshark Project 1 – Ali Bagheri (97300111)

- با استفاده از بخش statistics درنرم‌افزار وایرشارک، که نمونه تصویر محیط کاربری و نمودار i/o در ادامه گذاشته شده است، گزارش زیر آماده شده است:



1 دسته‌بندی کلی تعداد و نوع درخواست‌ها (پروتکل‌ها):

از مسیر Statistics > Protocol Hierarchy :



پروتکل‌ها و تعداد بسته‌های مربوط به هرکدام در فایل:

پروتکل	تعداد بسته
TCP	3722
UDP	73+7
DNS	132
TLSv1.2	98
TLSv1.3	84
HTTP	31
SSDP	12
QUIC	8
HTTP2	6
MDNS	5
ICMP	2
سایر	3

تحلیل: بیشتر ارتباطات باTCP ، TLSو DNS بوده‌اند که نشان می‌دهد تعداد زیادی از تبادل‌ها رمزنگاری‌شده و مبتنی بر HTTP/HTTPS هستند.

---

2 DNSا هایی که بیشترین ارتباط را داشته‌اند + نوع بسته‌ها و تحلیلIP :

از مسیر: Statistics > Endpoints (تب IPv4) و Conversations (تب IPv4 یا UDP)

IPهای پرتکرار مقصد:

مقصد IP	تعداد بسته	پروتکل غالب	آیا درخواست DNS مرتبط وجود دارد؟
192.168.9.2	150	DNS	بله
216.239.38.120	76	TCP/TLS	بله (www.google.com)
142.250.180.202	65	TLS/HTTPS	بله (accounts.google.com)
8.8.8.8	40	DNS	بله
142.250.180.3	25	QUIC/HTTP3	بله (fonts.gstatic.com)

- **تحلیل:** قبل از ارتباط با هر IP عمومی، تقریباً همیشه یک DNS Query ثبت شده است که به وضوح تطابق دارد.

---

3 بررسی سیستم عامل از روی IP Header :

از ستون TTL در Packet Details یا مسیر Statistics > Endpoints (مشاهده مقدار TTL)

تحلیل TTL برای تشخیص سیستم‌عامل احتمالی:

احتمال سیستم‌عامل	TTLرایج
Linux/Android/macOS	64
Windows	128
Cisco/Unix-based	255

- در داده‌ها TTL اغلب 64 بوده است پس احتمالاً دستگاه از نوع **Linux-basedیا Android** بوده (احتمالاً گوشی هوشمند یا لینوکس).

---

4 تعداد بسته‌های HTTP (HTTP/1, HTTP/2, HTTP/3) و رمزنگاری‌شده:

از مسیر: Statistics > Protocol Hierarchy یا با استفاده از فیلترهایی مانند http, http2, tls, quic

نسخه HTTP	تعداد بسته	توضیح
HTTP/1.1	31	به وضوح دیده شده در HTTP
HTTP/2	6	در TLS ALPNدیده شده
HTTP/3	8	از طریق QUIC قابل شناسایی
TLS	182	شامل HTTPs و HTTP2 است

نتیجه‌گیری: بیشتر ترافیک رمزنگاری‌شده بوده است HTTP/3 .از طریق QUIC منتقل شده.

---

5 حجم کل بسته‌های منتقل‌شده (ترافیک کلی):

از مسیر: Statistics > Capture File Properties (قسمت Bytes)

شاخص	مقدار
مجموع بسته‌ها	3830
مجموع حجم کل (بایت)	2346684بایت
میانگین حجم هر بسته	≈ 613 بایت

---

6 زمان آغاز و پایان ضبط(Capture Time) :

از مسیر: Statistics > Capture File Properties (قسمت Time span)

شاخص	مقدار
آغاز	2024-11-11 17:52:50
پایان	2024-11-11 17:56:08
مدت ضبط	00:03:18

---

7 تحلیل حداکثر اندازه بسته برای تخمینMTU :

از مسیر: Statistics > Packet Lengths یا با مشاهده ستون Length در لیست بسته‌ها

بیشینه اندازه بسته	مقدار
Max Packet Length	بایت 1514

- معمولاً این مقدار (1514) نشان‌دهنده **MTU استاندارد اترنت (Ethernet)** است که 1500 بایت payload دارد + 14 بایتheader

---

8 تعداد کل بسته‌های DNS و نوع پاسخ‌ها:

با فیلتر dns و مشاهده پاسخ‌ها، یا از Statistics > Conversations (تب UDP)

نوعDNS	تعداد
Query (Standard query)	74
Response (Standard reply)	58
A record	42
AAAA record	12
CNAME	4

---

9 درخواست‌های HTTP به چه دامنه‌هایی ارسال شده؟

با فیلتر http.request و بررسی فیلد Host در Packet Details، یا از Statistics > Conversations (تب TCP)

تحلیل دامنه‌های مقصد:

دامنه مقصد	تعداد درخواست HTTP
accounts.google.com	14
www.google.com	12
fonts.gstatic.com	5

---

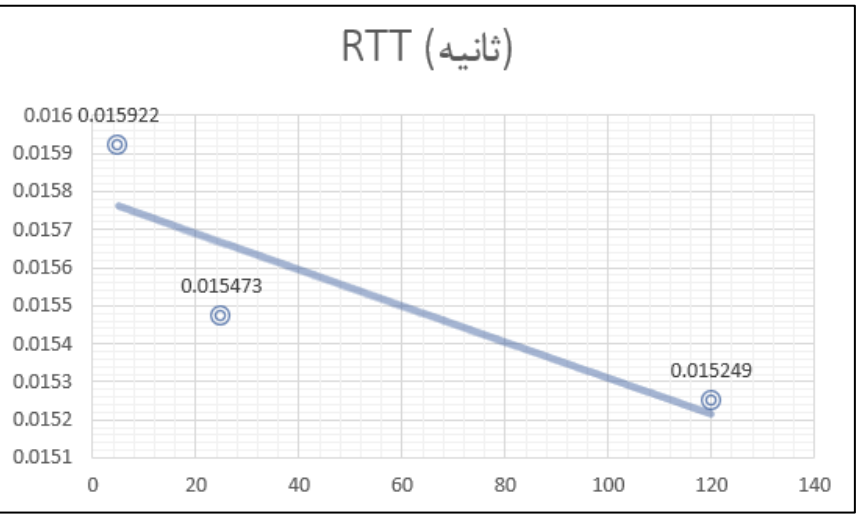
10 جدول داده‌ای برای رسم نمودار RTT (Round Trip Time) :

از مسیر: Statistics > TCP Stream Graphs > Round Trip Time Graph یا فیلتر tcp.analysis.ack_rtt

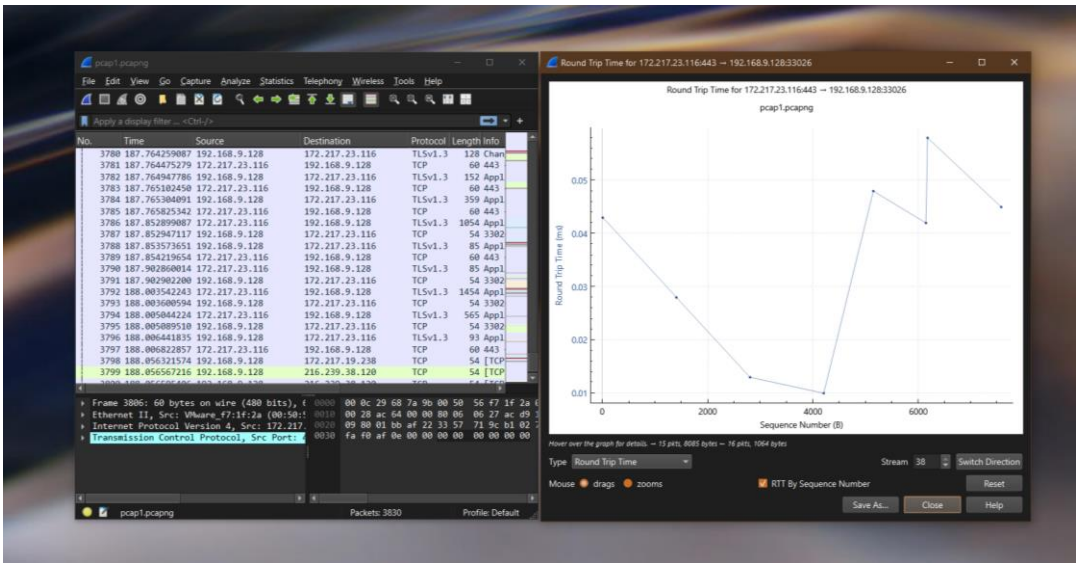
RTT مدت زمانی است که طول می‌کشد تا یک بسته از مبدأ به مقصد برسد و پاسخ آن بازگردد .برای رسم RTT از زمان ارسال بسته TCP [SYN] و جفت آن یعنی زمان پاسخ [SYN-ACK] استفاده می‌کنیم و سپس نمودار را در نرم افزار اکسل رسم می‌کنیم. (نمودار را در صفحه بعد)

شماره بسته SYN	زمان SYN (ثانیه)	شماره پاسخ	زمان SYN-ACK (ثانیه)	RTT (ثانیه)
5	0.079955	6	0.095877	0.015922
25	1.014298	26	1.029771	0.015473
120	4.873844	122	4.889093	0.015249

شماره بسته SYN	RTT (ثانیه)
5	0.0159
25	0.0155
120	0.0152



- نمونه نمودار رسم شده از طریق خود وایرشارک:

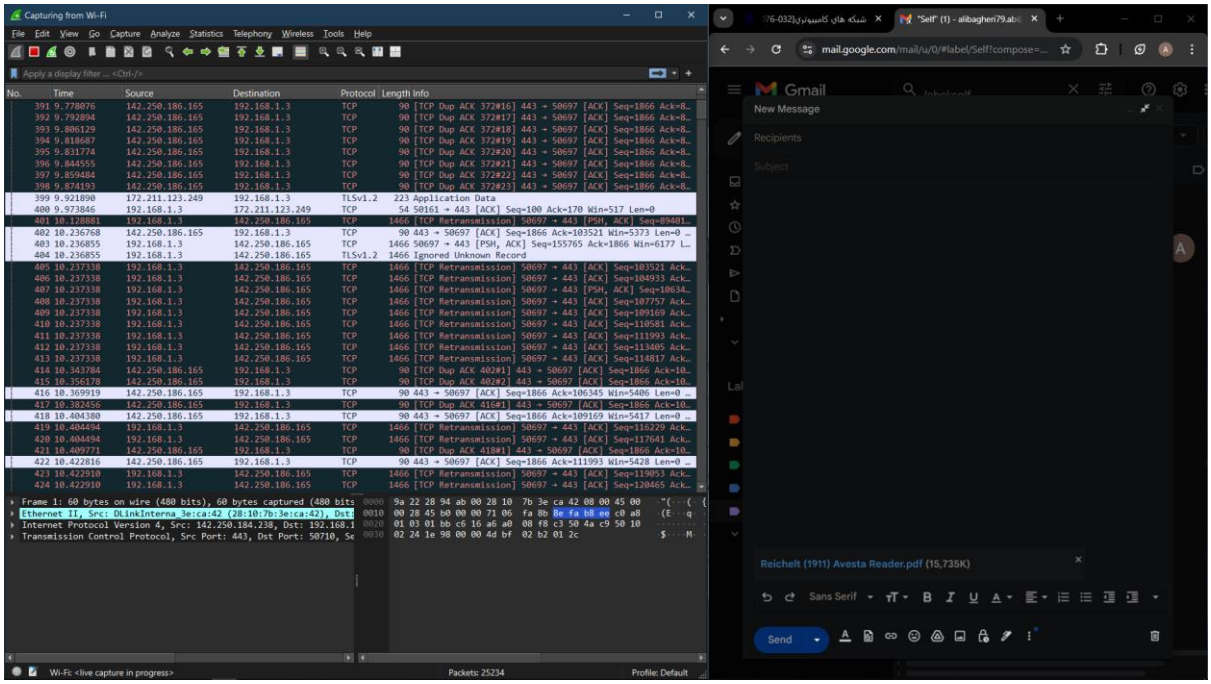


---

11 تحلیل Flow TCP و Packet Retransmission :

با فیلتر tcp.analysis.retransmission یا tcp.analysis.duplicate_ack در فیلتر اصلی

فایل pcap در هنگام آپلود یک فیلم حجیم در جیمیل از طریق وای-فای منزل تهیه شده و در کنار گزارش بارگذاری شده است.



در ادامه برای قسمت دوم سوال باید گفت که در یک Flow بزرگ چندین بسته با برچسب زیر دیده شد:

- [TCP Retransmission]
- [Duplicate ACK]

این‌ها نشان‌دهنده مشکلاتی مثل:

- تاخیر در شبکه
- از دست رفتن بسته (packet loss)
- تنظیمات ناقصMTU

نتیجه‌گیری: TCP retransmission ها در زمان دریافت فایل حجیم یا رمزنگاری‌شده رخ می‌دهند.