



دانشگاه صنعتی شریف

دانشکده مهندسی کامپیوتر

گزارش کار آزمایشگاه

آزمایشگاه شبکه های کامپیوتری

گزارش آزمایش شماره ۲

شماره گروه: ۴

ارشیا یوسف نیا ۴۰۱۱۰۴۱۵

محمد فرهان بهرامی ۴۰۱۱۰۵۷۲۹

امیر مهدی دارابی ۹۹۱۰۵۴۳۱

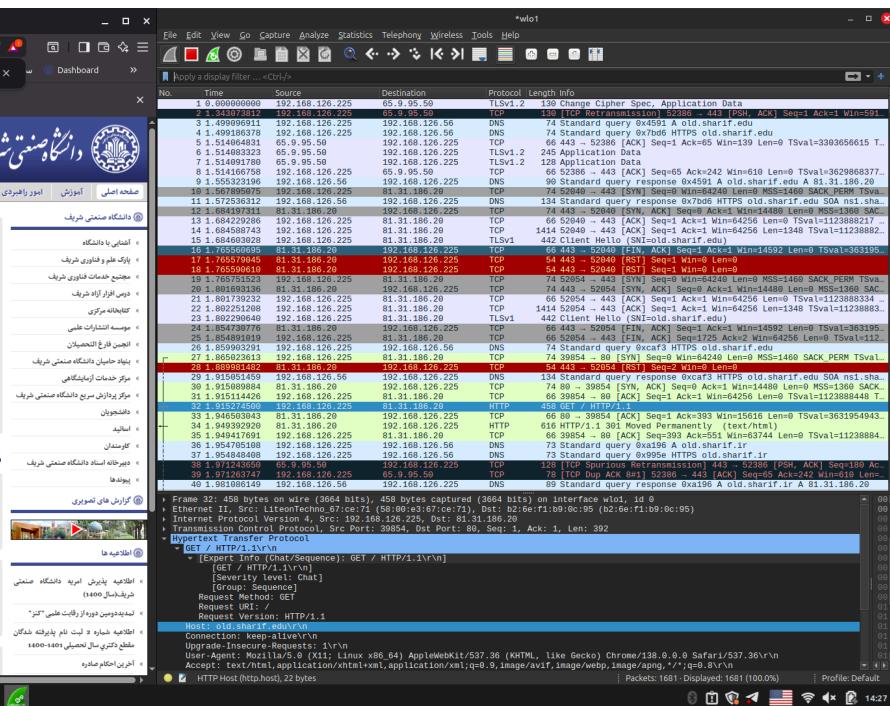
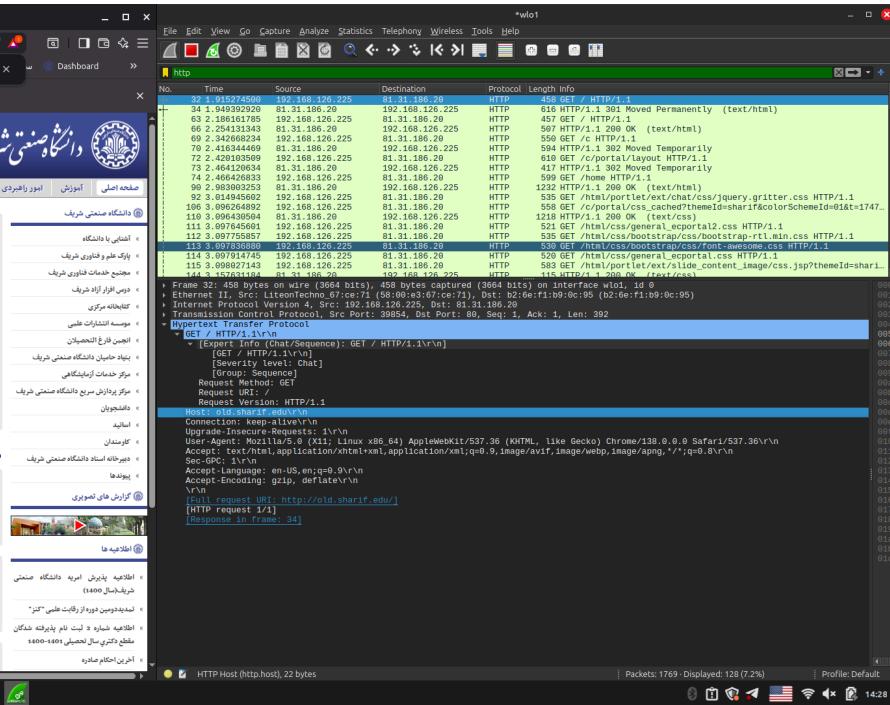
استاد درس: دکتر صفائی

تاریخ: تابستان ۱۴۰۰

بخش اول

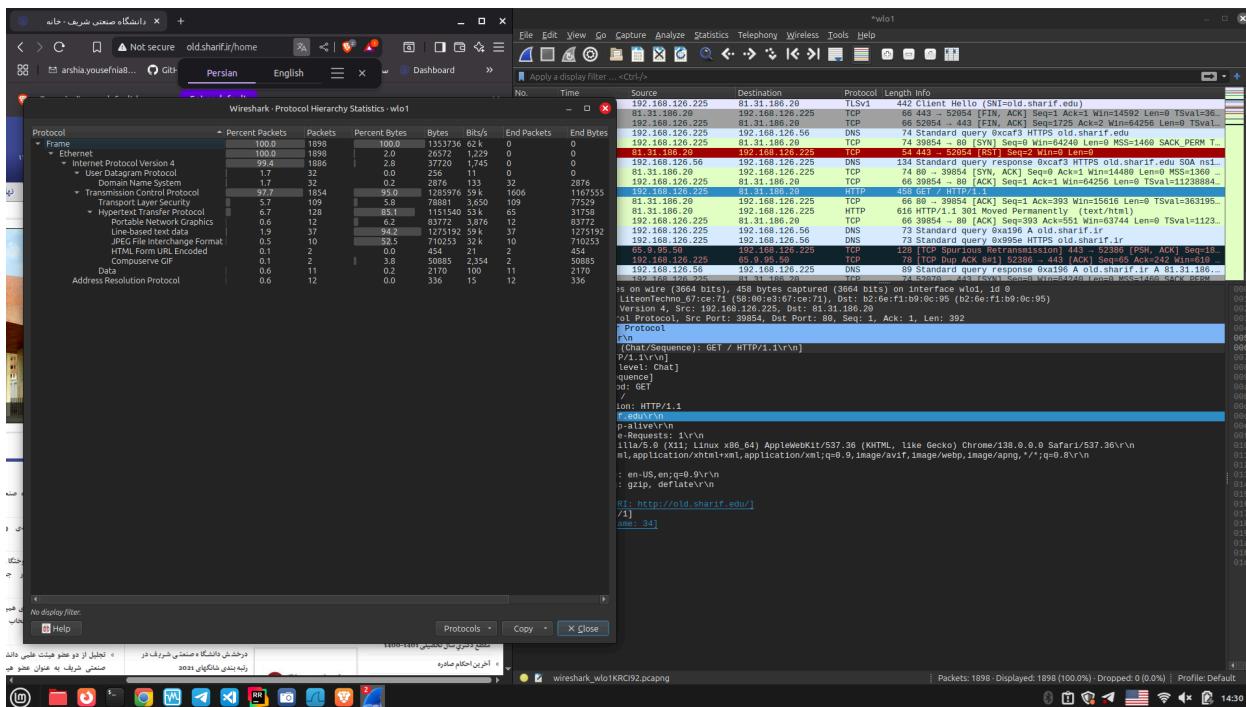
برای این بخش از سایت old.sharif.ir استفاده کردیم.

همانطور که در تصاویر زیر مشاهده می‌کنید، دو نمونه بازیابی از صفحه اول این سایت را در کنار داده‌های Wireshark در اختیار داریم:



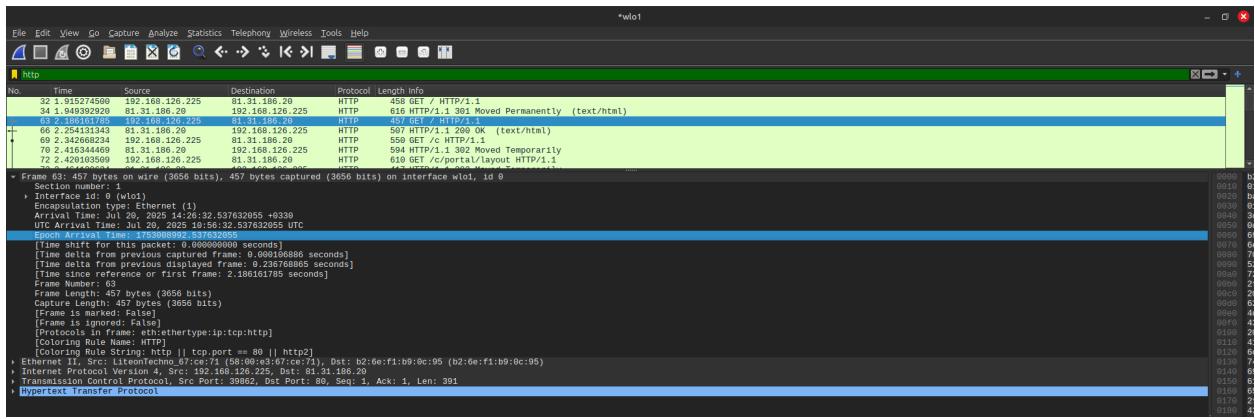
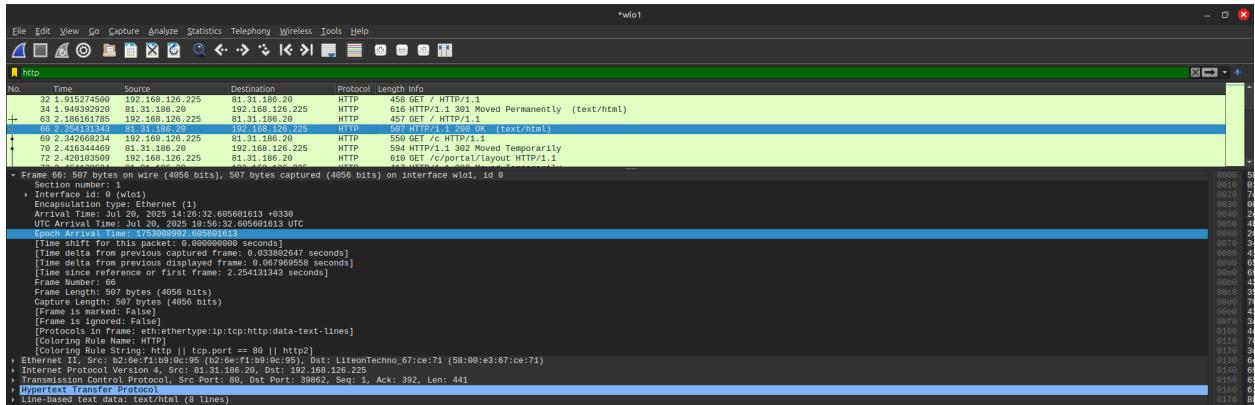
۱. در ادامه نگاهی به داده‌های آماری که Wireshark در اختیار ما می‌گذارد را بررسی می‌کنیم.

مطابق تصویر زیر پرکاربردترین پروتکل لایه شبکه IPv4، پرکاربردترین پروتکل لایه انتقال TCP و پرکاربردترین پروتکل لایه کاربرد HTTP می‌باشد. همچنین مشاهده می‌شود که در زیرشاخه پروتکل‌های لایه کاربرد وابسته به UDP پرکاربردترین پروتکل DNS است.

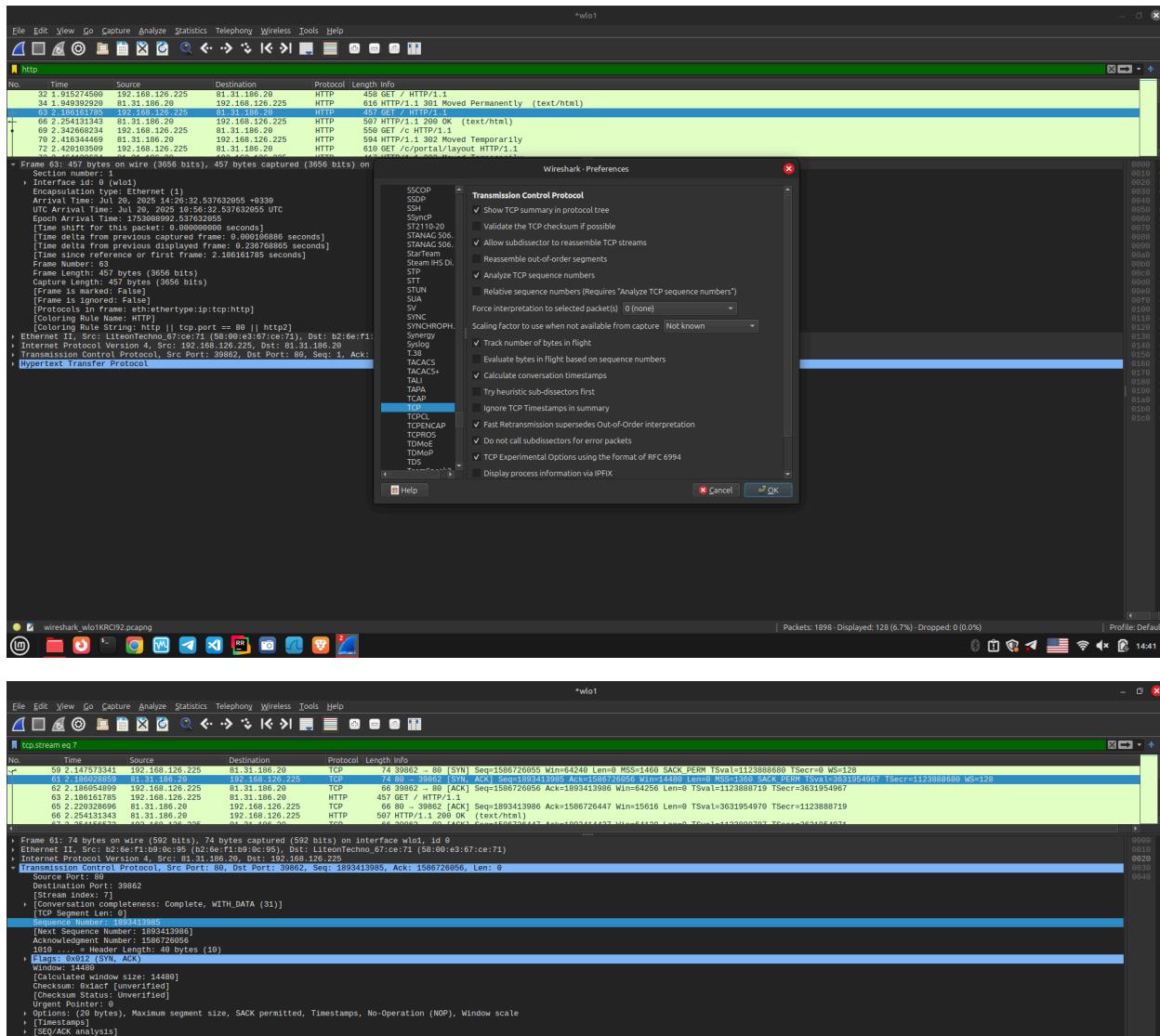


۲. مطابق دو تصویر پایین، درخواست HTTP GET در زمان 1753008992.537632055 ارسال و پاسخ متناظر با آن در زمان 1753008992.605601613 آمده که فاصله زمان این دو برابر با مقدار زیر است:

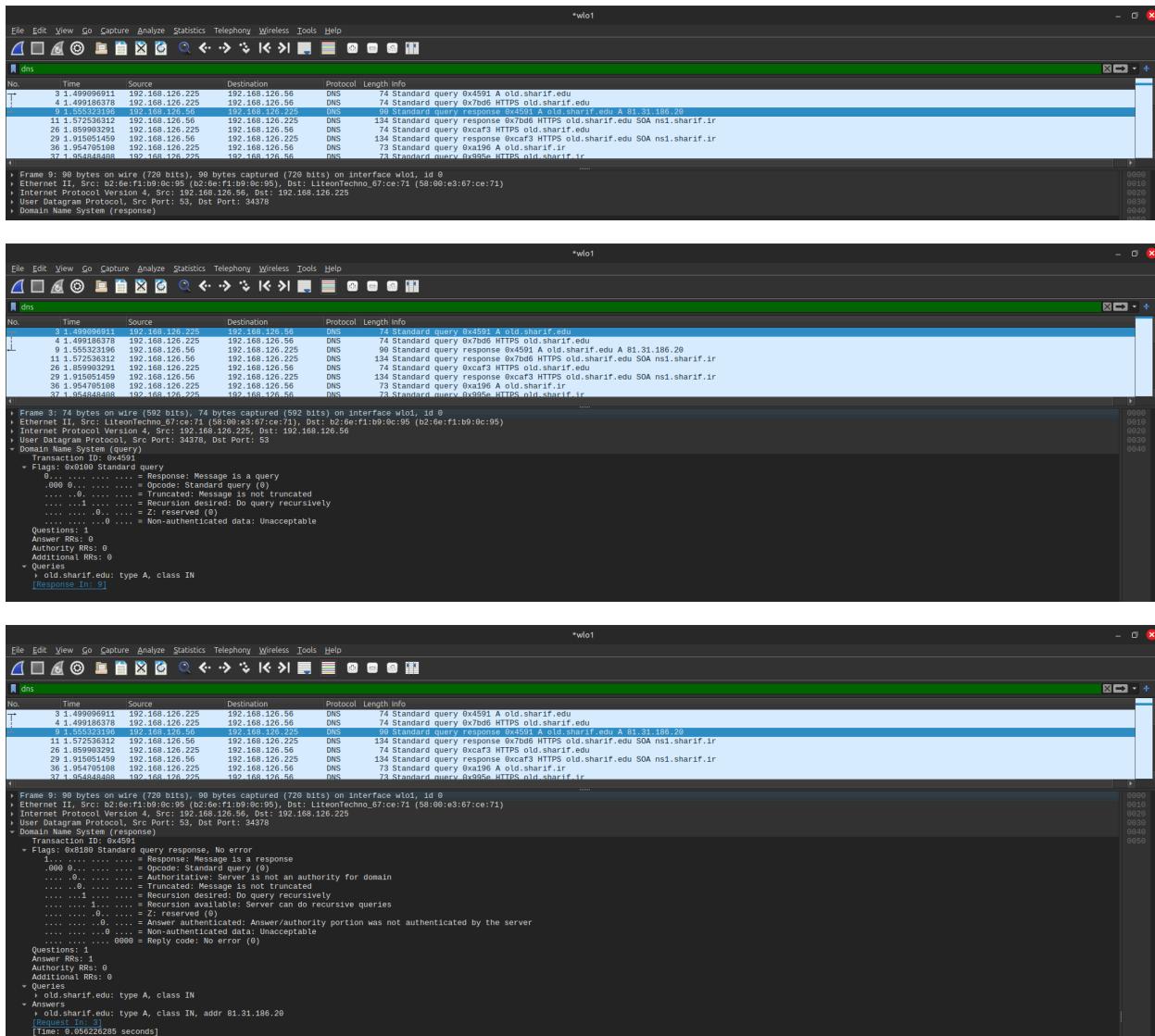
$$1753008992.605601613 - 1753008992.537632055 = 0.67969558\text{s}$$



برای یافتن شماره ترتیب، از **TCP -> Preferences** و قسمت پروتکل TCP حالت شماره‌گذاری نسیی را خاموش می‌کنیم و سپس بر روی اولین درخواست HTTP ارسال شده کلیک راست کرده و **Follow** و **حالت TCP Stream** را انتخاب کرده تا بسته‌های TCP مربوط به آن را پیدا کنیم. سپس با یافتن اولین بسته SYN ارسال شده به جواب مدنظر می‌رسیم. همانطور که تصویر زیر پیداست شماره ترتیب برابر 1893413985 است.

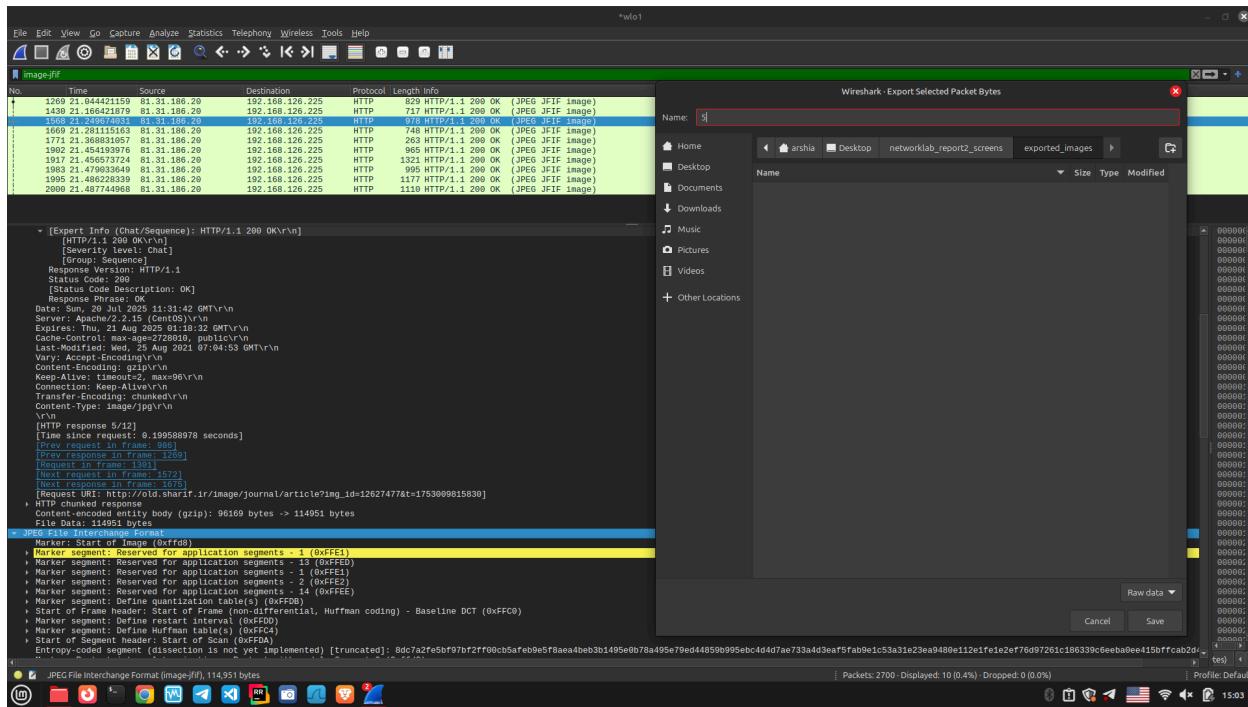


۳. مطابق تصاویر زیر یک DNS Query به شکل استاندارد و از نوع A به معنی Authoritative بر پستر پروتکل UDP (تصویر اول) ارسال شده است و پاسخ آن هم به صورت استاندارد و از نوع A بر همین پستر و با IP Address: 81.31.186.20 (تصاویر دوم و سوم) دریافت شده است.

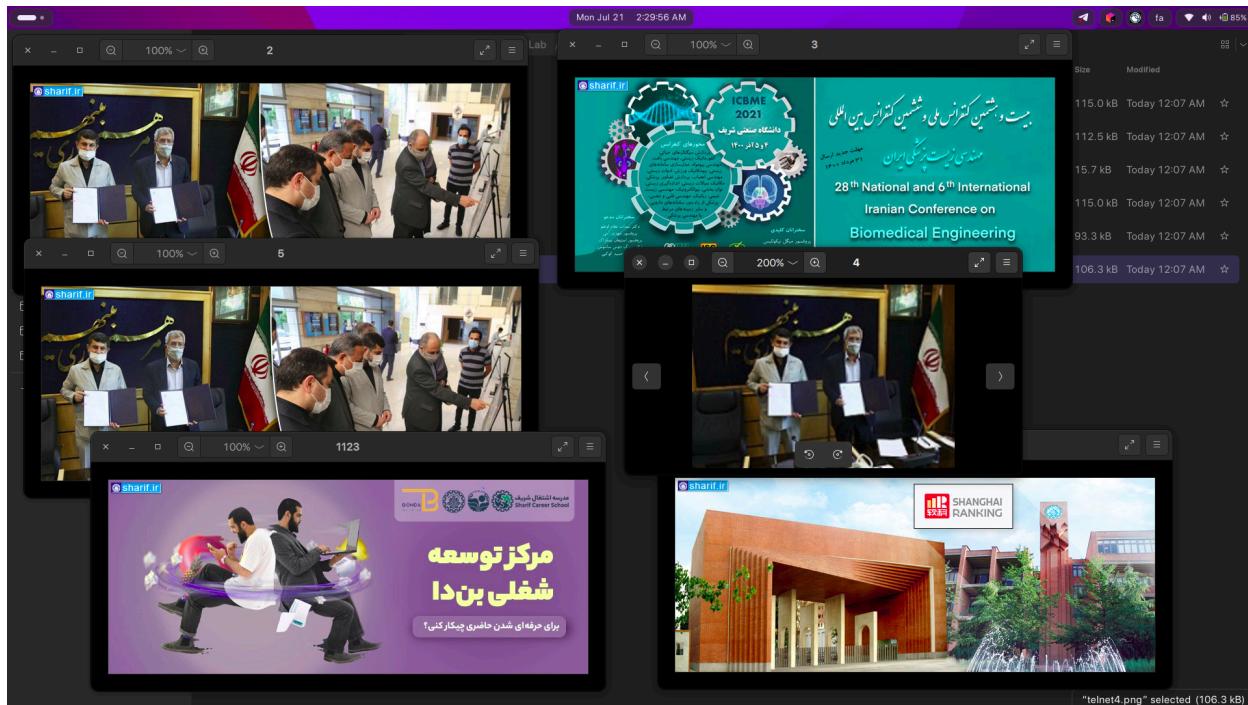


۴. برای مشاهده تصاویر فیلتر `image-jfif` را روی WireShark اعمال می‌کنیم.

سپس هر یک از عکس‌ها را انتخاب کرده و با کلیک راست روی عکس‌ها Export Packet Bytes و انتخاب

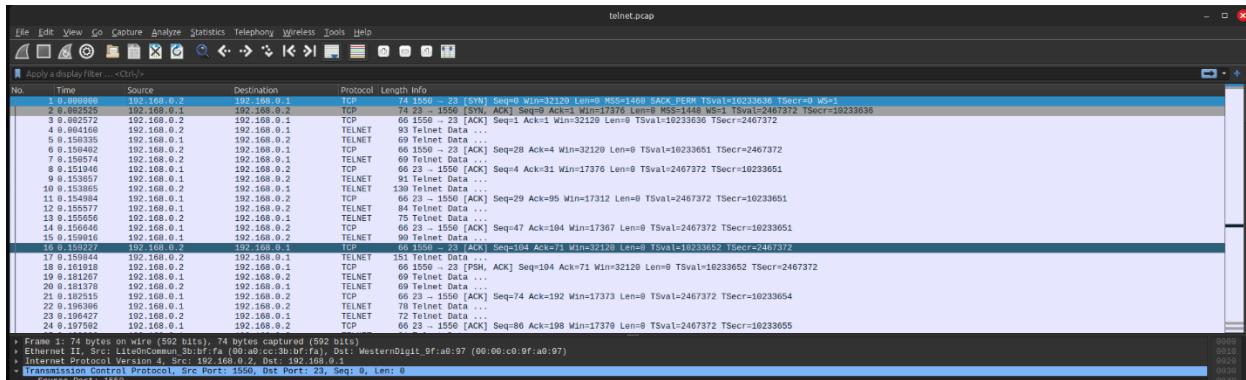


تصاویر export شده:



بخش دوم

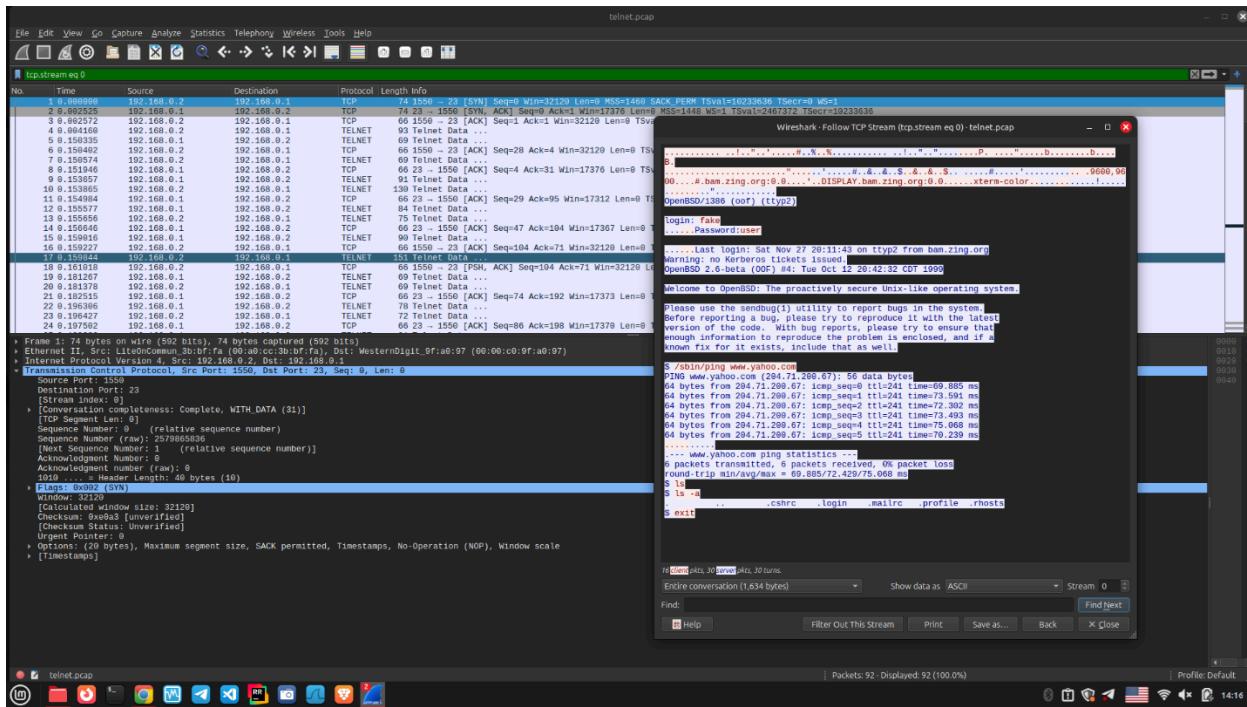
۱. همانطور که در تصویر ۱ مشاهده می‌شود، آدرس IP مربوط به کلاینت ۱۹۲.۱۶۸.۰.۲ می‌باشد و همچنین آدرس IP مربوط به سرور نیز ۱۹۲.۱۶۸.۰.۱ می‌باشد.



تصویر ۱) وضعیت بسته‌های ارسال شده Telnet

برای سوالات بعدی، باید بسته‌هایی با پروتکل TELNET را فیلتر کنیم.

برای این کار باید در قسمت بالا یعنی "Apply a display filter", tcp.stream eq 0" را اعمال کرده و تمامی اطلاعات فرستاده و گرفته شده مثل تصویر ۲ قابل مشاهده است.



تصویر 2) محتوای اطلاعات فرستاده و گرفته شده در Telnet

.۲. همانطور که در تصویر ۳ مشاهده می‌کنید، رمز عبور کلاینت بازیابی شده user است.

```

login: fake
.....Password:user

.....Last login: Sat Nov 27 20:11:43 on ttys0 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

```

تصویر 3) رمز عبور بازیابی شده کلاینت

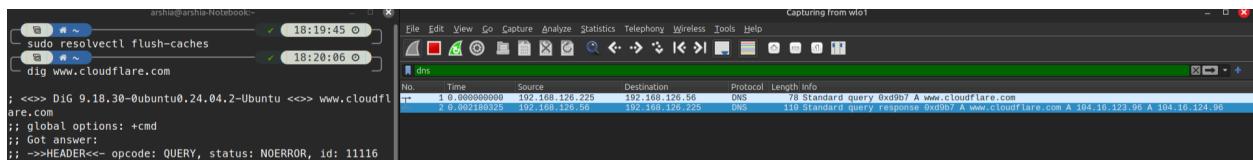
۳. در تصویر ۴ دستورات اجرا شده توسط کلاینت قابل مشاهده است. دستورات با \$ شروع شده و با رنگ قرمز می‌باشند.

```
$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
.....
--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$ ls
$ ls -a
. .. .cshrc .login .mailrc .profile .rhosts
$ exit
```

تصویر ۴) دستورات استفاده شده توسط کلاینت

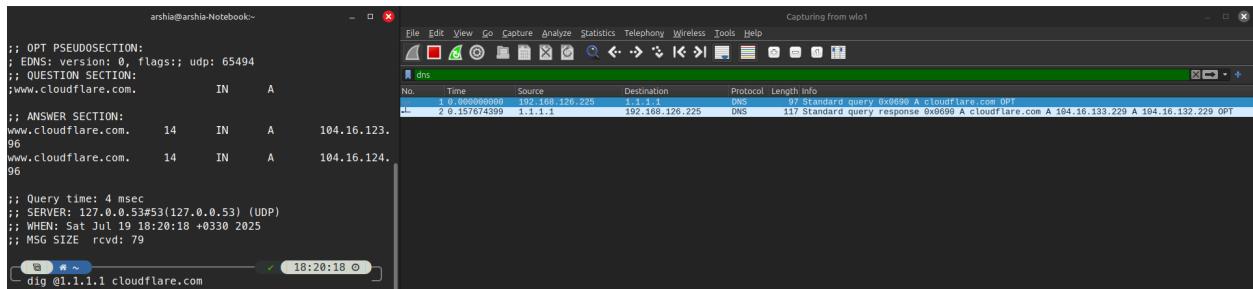
بخش سوم

۱. ما تصمیم گرفتیم که برای اجرای دستور dig، از سایت www.cloudflare.com استفاده کنیم.
همانطور که در تصویر ۵ قابل مشاهده است، query برای DNS server محلی با آدرس ۱۹۲.۱۶۸.۱۲۶.۵۶ ارسال شده است.



تصویر ۵) ارسال query با دستور dig www.cloudflare.com

اما اگر از دستور dig @1.1.1.1 استفاده کنیم، این برای DNS Server های query می شود، که در تصویر ۶ قابل مشاهده است.



تصویر ۶) ارسال query با دستور dig @1.1.1.1 www.cloudflare.com

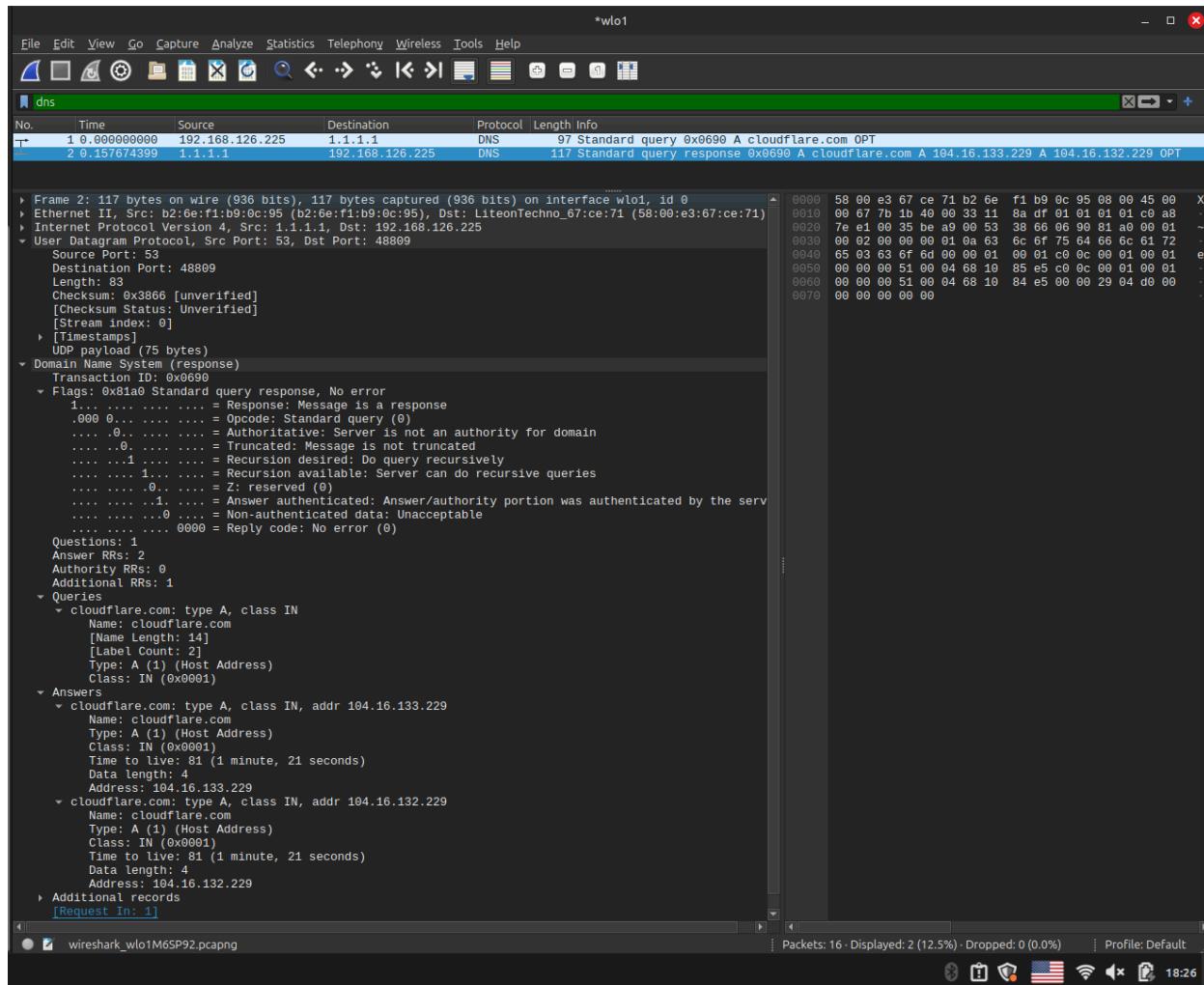
۲. در تصویر ۷، دو بسته‌ی مربوط به پروتکل DNS دیده می‌شود که یکی مربوط به درخواست (Query) و دیگری مربوط به پاسخ (Response) است.

در بسته اول، کامپیوتر کلاینت با آدرس IP محلی 192.168.126.225 درخواست خود را به سرور DNS با آدرس IP 1.1.1.1 که برای Cloudflare است، ارسال کرده است. این درخواست شامل یک Transaction ID با Query می‌باشد. در قسمت flags این بسته، مقدار 0x0100 دیده می‌شود که نشان می‌دهد این یک درخواست استاندارد (Standard Query) است و همچنین درخواست بازگشتی (Recursion Desired) فعال است. بازگشت‌پذیری یعنی از سرور DNS خواسته می‌شود تا اگر پاسخ را در حافظه کش خود ندارد، خودش به جای کلاینت جست‌وجو را تا یافتن پاسخ نهایی ادامه دهد.

در بخش Query این بسته، دامنه‌ای که برای آن درخواست ارسال شده، یعنی cloudflare.com، با نوع رکورد A مشخص شده است. نوع A به این معنایست که کلاینت به دنبال آدرس IPv4 این دامنه است و کلاس IN نیز نشان‌دهنده این است که درخواست مربوط به اینترنت عمومی است.

بسته دوم پاسخ سرور DNS است که از همان آدرس 1.1.1.1 به مقصد کلاینت ارسال شده و دارای همان Transaction ID (یعنی 0x0690) است که برای تطابق با درخواست اولیه استفاده می‌شود. این بسته نیز دارای ساختار DNS استاندارد است و در قسمت Flags مقدار 0x8180 دیده می‌شود که نشان‌دهنده یک پاسخ معتبر بدون خطأ است. در این بسته گزینه Recursion Available فعال است، به این معنا که سرور از قابلیت جست‌وجوی بازگشتی پشتیبانی می‌کند.

در پاسخ دریافتی دو رکورد از نوع A بازگردانده شده است. هر دوی این رکوردها مربوط به دامنه cloudflare.com هستند و دو آدرس IP مختلف برای آن ارائه شده‌اند: یکی 104.16.133.229 و دیگری 104.16.132.229. این موضوع معمولاً به دلایل توازن بار (Load Balancing) و افزونگی (Redundancy) انجام می‌شود. همچنین هر کدام از این رکوردها دارای مدت زمان اعتبار (TTL) برابر با 81 ثانیه هستند که نشان می‌دهد کلاینت می‌تواند تا 81 ثانیه این پاسخ را در کش خود نگه دارد بدون آنکه دوباره درخواست جدیدی به سرور ارسال کند.



تصویر ۷) درخواست و پاسخ گرفته شده DNS

منابع

<https://www.youtube.com/watch?v=pGyH67K41ro>