آز شبکه

نیم‌سال اول ۰۱-۰۲

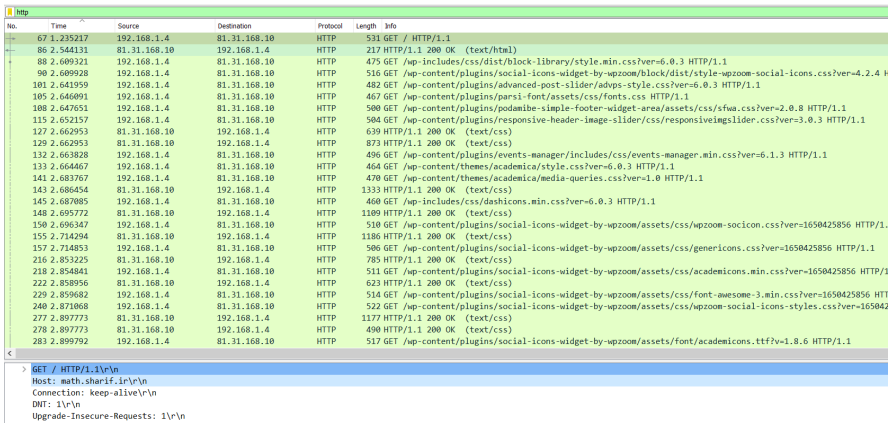
مدرس: دکتر صفائی

دانشکده مهندسی کامپیوتر

عماد زین‌اوقلی	پارسا رییسی	سیدابوالفضل رحیمی
۹۸۱۰۳۲۶۷	۹۸۱۰۳۲۲۳	۹۷۱۰۵۹۴۱

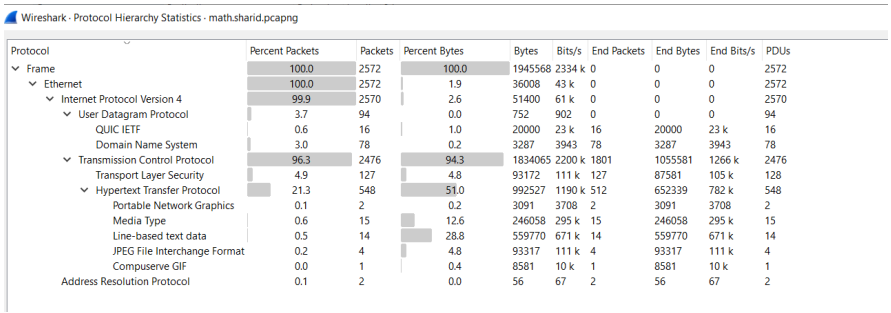
۱ HTTP

سایت `math.sharif.ir` باز کردیم و نتایج زیر ۲ را گرفتیم.



شکل ۱: فیلتر بر حسب پروتکل HTTP

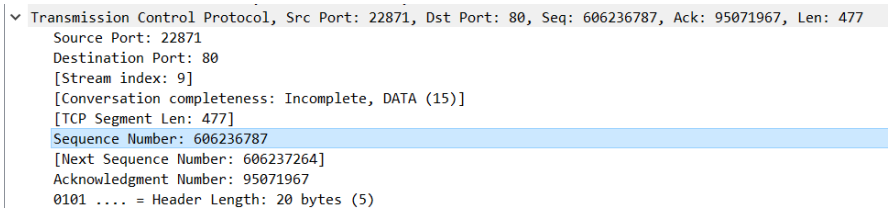
۱. ابزار آماری wireshark خروجی زیر ۲ را داده است.



شکل ۲: تفکیک بر اساس پروتکل‌ها

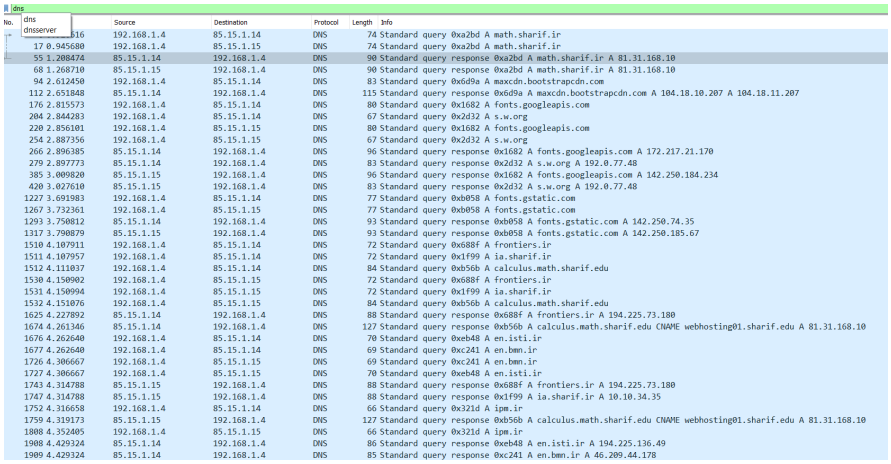
۲. با توجه به ۲ فاصله زمانی بین درخواست تا پاسخ برابر با 1.3 ثانیه بوده است.

۳. ابتدا بایستی چک‌باکس relative sequence number در preferences را خاموش کنیم. سپس با توجه به ۳ شماره اولین درخواست TCP برابر با 606236787 است.



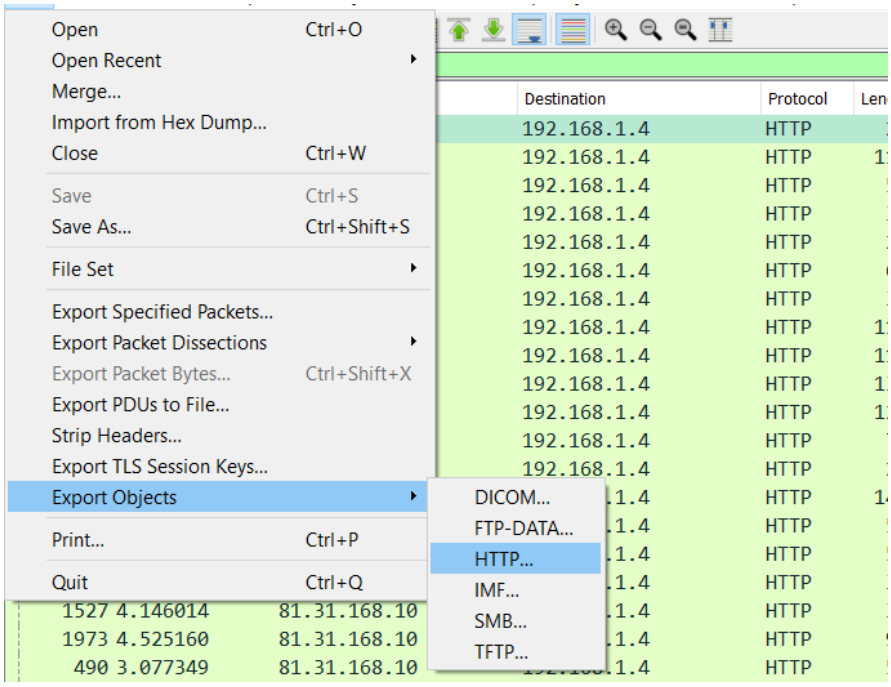
شکل ۳: اولین درخواست TCP

۴. با فیلتر کردن بر حسب پروتکل DNS ۴ در می‌یابیم که اکثر درخواست‌ها از نوع A بوده است.



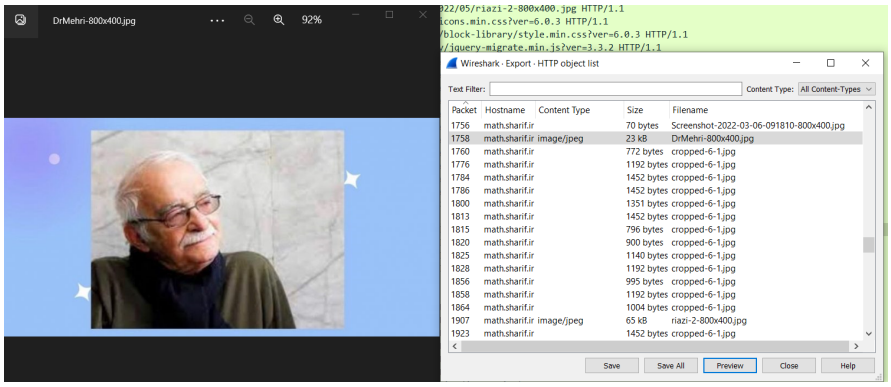
شکل ۴: فیلتر بر حسب پروتکل DNS

۵. گزینه `Export Objects: HTTP` را از منو ۵ انتخاب می‌کنیم.

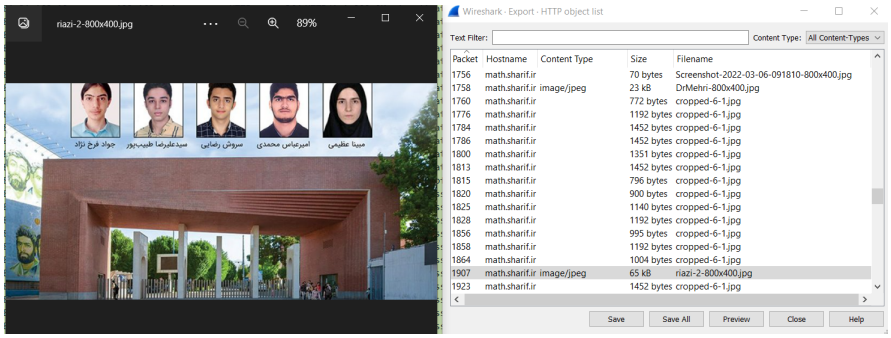


شکل ۵: `Export Objects: HTTP`

دو نمونه زیر را انتخاب کردیم.



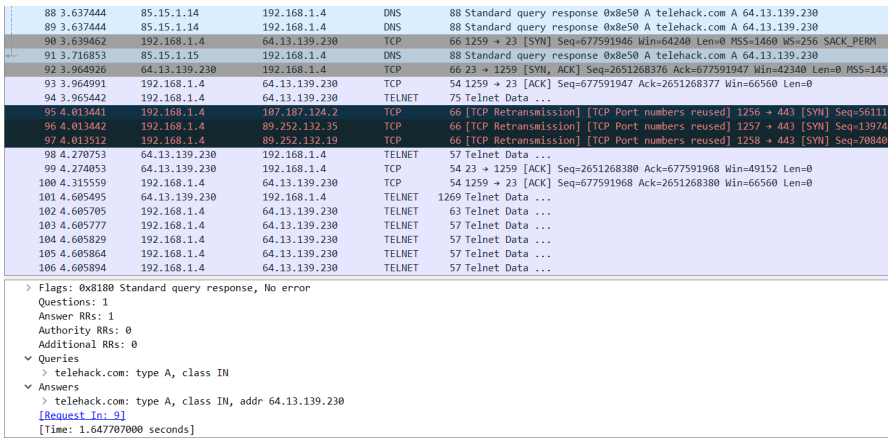
شکل ۶: نمونه اول



شکل ۷: نمونه دوم

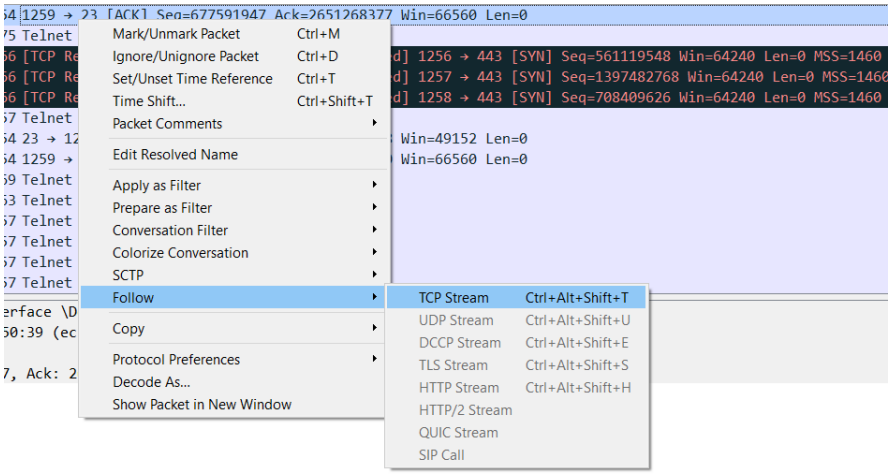
۲ Telnet

۱. با توجه به جواب DNS می‌فهمیم که IP آدرس سرور 230.139.13.64 و آدرس کلاینت 4.1.168.192 است.



شکل ۸: IP Address

۲. با استفاده از قابلیت Follow TCP Stream ۹ می‌توان حرف فرستاده و گرفته شده را مشاهده کرد.



شکل ۹: Follow TCP Stream

شکل ۱۰: ارتباط Telnet

مشاهده می‌کنیم که `username: eiou` و `password: eiouxz` است.

۳. با توجه به ۱۰ دستورات فرستاده شده `login`، `joke`، `rand`، `exit` بودند.

۳ DNS

آزمایش را با سایت `sharif.ir` انجام دادیم.

```
C:\WINDOWS\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\WINDOWS\system32>nslookup sharif.ir
Server:  UnKnown
Address:  85.15.1.14

Non-authoritative answer:
Name:    sharif.ir
Address:  152.89.13.54
```

شکل ۱۱: `nslookup sharif.ir`

No.	Time	Source	Destination	Protocol	Length	Info
3	2.630994	192.168.1.4	85.15.1.14	DNS	83	Standard query 0x0001 PTR 14.1.15.85.in-addr.arpa
4	2.657593	85.15.1.14	192.168.1.4	DNS	83	Standard query response 0x0001 No such name PTR 14.1.15.85.in-addr.arpa
5	2.658988	192.168.1.4	85.15.1.14	DNS	69	Standard query 0x0002 A sharif.ir
6	2.956249	85.15.1.14	192.168.1.4	DNS	85	Standard query response 0x0002 A sharif.ir A 152.89.13.54
7	2.958690	192.168.1.4	85.15.1.14	DNS	69	Standard query 0x0003 AAAA sharif.ir
8	3.134169	85.15.1.14	192.168.1.4	DNS	120	Standard query response 0x0003 AAAA sharif.ir SOA ns1.sharif.ir

شکل ۱۲: فیلتر برحسب DNS

۱. با توجه به ۱۱ و ۱۲ در می‌یابیم که درخواست‌ها به و پاسخ‌ها از سرور `14.1.15.85` ارسال می‌شوند.

۲. هدرهای درخواست و پاسخ DNS به صورت زیر ۱۳،۱۴ هستند.

```
▾ Domain Name System (query)
    Transaction ID: 0x0002
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    › sharif.ir: type A, class IN
    [Response In: 6]
```

شکل ۱۳: درخواست DNS

flag های هدر به ترتیب مشخص شده‌اند:

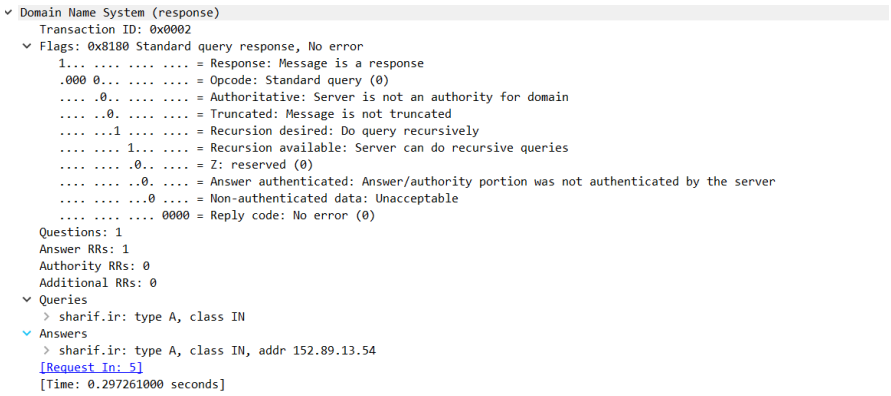
نوع پیام این پیام یک درخواست است.

نوع درخواست یک درخواست استاندارد است.

پیام خرد شده است؟ خیر، زیرا درخواست بزرگ نبوده است.

درخواست بازگشتی بله درخواست به صورت بازگشتی حل شود.

سپس تعداد درخواست‌ها و غیره مشخص شده‌اند. در نهایت، درخواست‌مان آمده است که از نوع A یعنی host address و کلاس IN یعنی internet است.



شکل ۱۴: پاسخ DNS

flag های هدر به ترتیب مشخص شده‌اند:

نوع پیام این پیام یک پاسخ است.

نوع درخواست یک درخواست استاندارد است.

آیا سرور Authoritative است؟ خیر.

پیام خرد شده است؟ خیر، زیرا پاسخ بزرگ نبوده است.

درخواست بازگشتی بله درخواست به صورت بازگشتی حل شود.

امکان درخواست بازگشتی بله سرور می‌تواند درخواست به صورت بازگشتی حل کند.

سپس تعداد درخواست‌ها و غیره مشخص شده‌اند. در نهایت، درخواست‌مان و پاسخ آن آمده است که از نوع A و کلاس IN است و آدرس آن 152.89.13.54 است.