آزمایشگاه شبکه‌های کامپیوتری

آزمایش دوم

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

نیم سال دوم ۰۱-۰۰

استاد:

جناب آقای دکتر صفایی

اعضای گروه:

محمدسپهر پورقناد - ۹۷۱۰۱۳۵۹

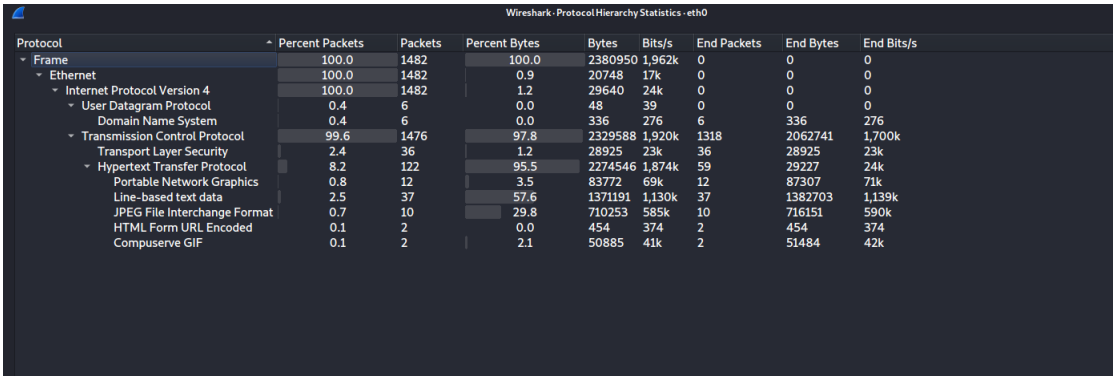
سپهر صفری - ۹۷۱۰۸۲۶۳

امیرمهدی نامجو - ۹۷۱۰۷۲۱۲

۱ سوالات بخش اول

ابتدا ذکر این نکته ضروری است که برای این بخش از سایت **old.sharif.ir** استفاده کردیم. دلیل این که از خود سایت اصلی شریف استفاده نکردیم این است که سایت جدید شریف تنها از طریق پروتکل **HTTPS** در دسترس است و بعضی از قسمت‌های تمرین، مثلا استخراج عکس‌ها به دلیل رمزنگاری اطلاعات و نیاز به رمزگشایی آنان کمی بیش از حد لازم پیچیده می‌شد.

۱. برای این قسمت از امکانات آماری (Statistics) نرم‌افزار وایرشارک استفاده می‌کنیم. مطابق شکل ۱ پرکاربردترین پروتکل لایه شبکه **IPV4** ، پرکاربردترین پروتکل لایه انتقال **TCP** و پر کاربردترین پروتکل لایه کاربرد **HTTP** بوده است. همچنین شاهد این هستیم که در زیر شاخه پروتکل‌های لایه کاربرد وابسته به **UDP** پرکابردترین (و تنها پروتکل) پروتکل **DNS** بوده است.



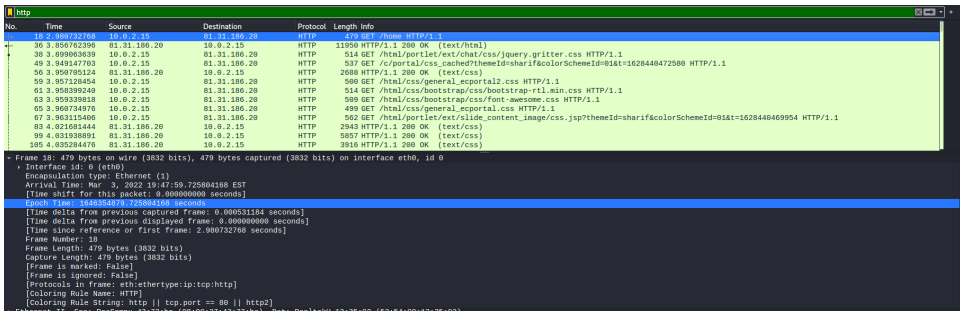
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	1482	100.0	2380950	1,962k	0	0	0
Ethernet	100.0	1482	0.9	20748	17k	0	0	0
Internet Protocol Version 4	100.0	1482	1.2	29640	24k	0	0	0
User Datagram Protocol	0.4	6	0.0	48	39	0	0	0
Domain Name System	0.4	6	0.0	336	276	6	336	276
Transmission Control Protocol	99.6	1476	97.8	2329588	1,920k	1318	2062741	1,700k
Transport Layer Security	2.4	36	1.2	28925	23k	36	28925	23k
Hypertext Transfer Protocol	8.2	122	95.5	2274546	1,874k	59	29227	24k
Portable Network Graphics	0.8	12	3.5	83772	69k	12	87307	71k
Line-based text data	2.5	37	57.6	1371191	1,130k	37	1382703	1,139k
JPEG File Interchange Format	0.7	10	29.8	710253	585k	10	716151	590k
HTML Form URL Encoded	0.1	2	0.0	454	374	2	454	374
Compuserve GIF	0.1	2	2.1	50885	41k	2	51484	42k

شکل ۱: درصد استفاده از هر یک از پروتکل‌ها

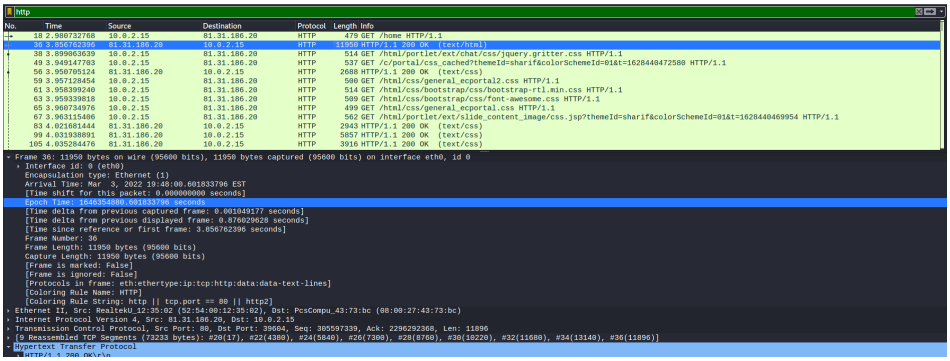
۲. مطابق دو شکل ۲ و ۳ درخواست **HTTP GET** در زمان 1646354879.725804168 ارسال شده و پاسخ آن در لحظه 1646354880.601833796 دریافت شده است. پس فاصله زمانی برابر

$$1646354880.601833796 - 1646354879.725804168 = 0.876029628s$$

است.

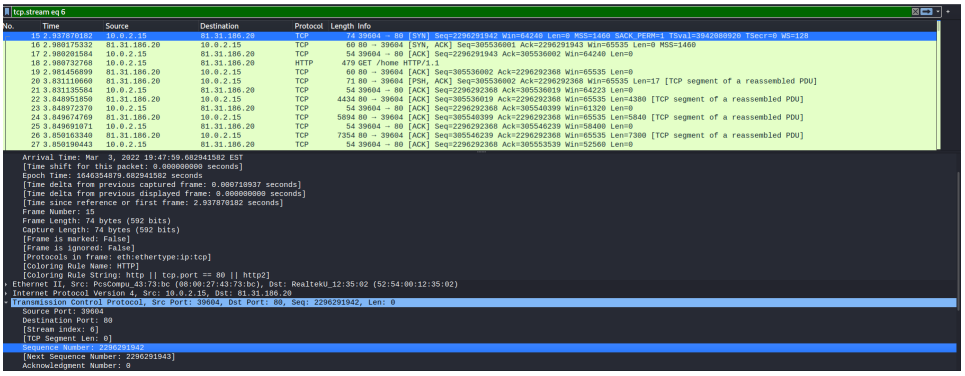


شکل ۲: اولین درخواست **HTTP GET**



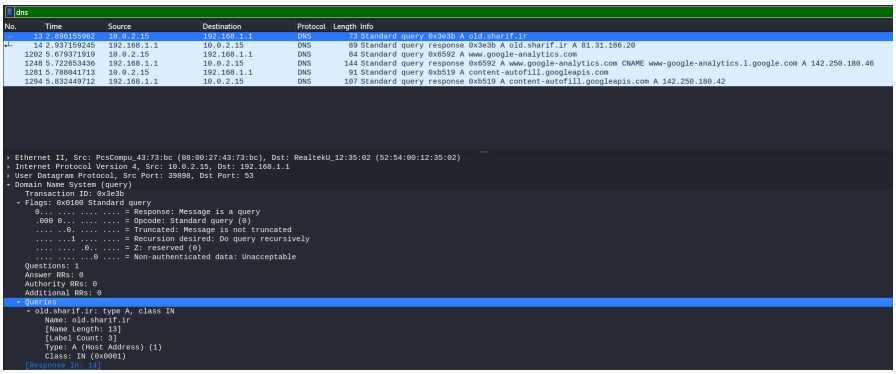
شکل ۳: پاسخ **HTTP OK** نظیر درخواست قبلی

برای بدست آوردن شماره ترتیب، از تنظیمات Preferences برنامه وایرشارک و قسمت پروتکل **TCP** ، حالت شماره‌گذاری نسبی را غیرفعال می‌کنیم. سپس بر روی اولین درخواست **HTTP** ارسال شده کلیک راست کرده و گزینه Follow و حالت **TCP Stream** را انتخاب می‌کنیم تا بسته‌های **TCP** مربوط به آن را بیابیم. با یافتن اولین بسته **SYN** ارسال شده به جواب می‌رسیم. جواب مطابق شکل ۴ بوده و در این جا شماره ترتیب مطلق برابر 2296291942 است.

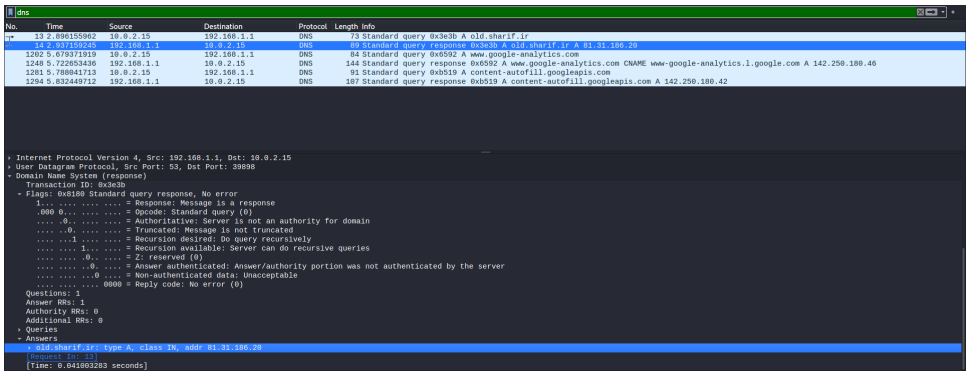


شکل ۴: اولین بسته **TCP SYN** نظیر درخواست قبلی

۳. مطابق شکل‌های ۵ و ٦ یک کوئری **DNS** به شکل استاندارد و از نوع **A** به معنی Authoritative بر بستر پروتکل UDP ارسال شده است و پاسخ آن هم به صورت استاندارد و از نوع **A** بر همین بستر و با آدرس آی‌پی **81.31.186.20** دریافت شده است.

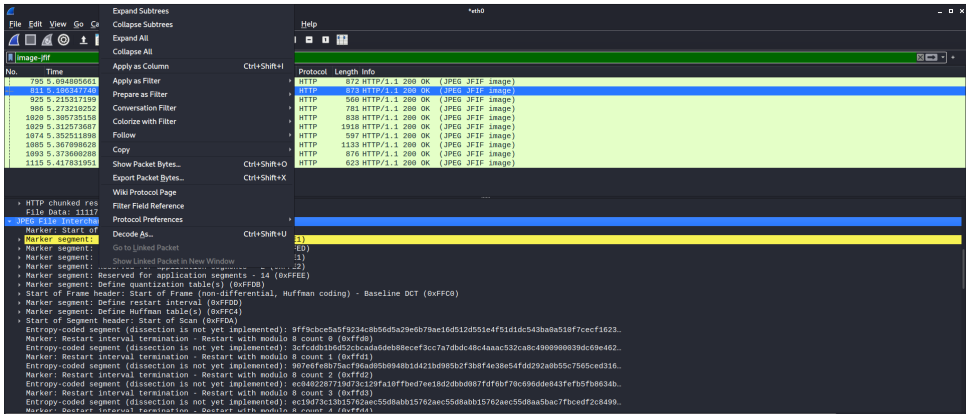


شکل ۵: کوئری **DNS**



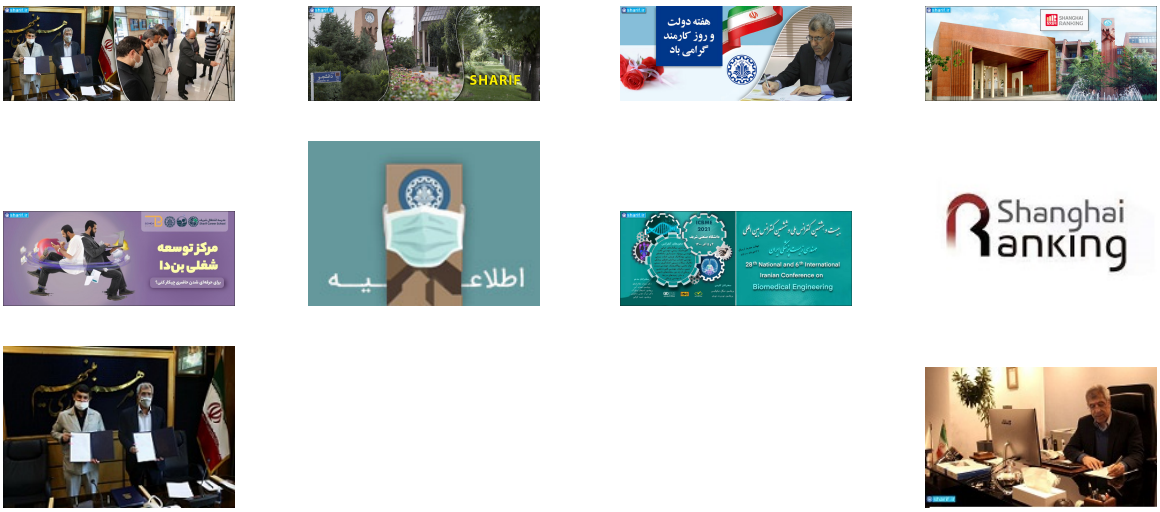
شکل ٦: پاسخ **DNS**

۴. مطابق شکل ۷ برای مشاهده عکس‌ها فیلتر **image-jfif** را روی وایرشارک اعمال می‌کنیم. سپس هر یک از عکس‌های را انتخاب کرده و با کلیک راست روی JPEG File Interchangeable Format و انتخاب Export Packet Bytes عکس‌ها را ذخیره می‌کنیم.



شکل ۷: مشاهده شکل‌های دانلود شده از سرور

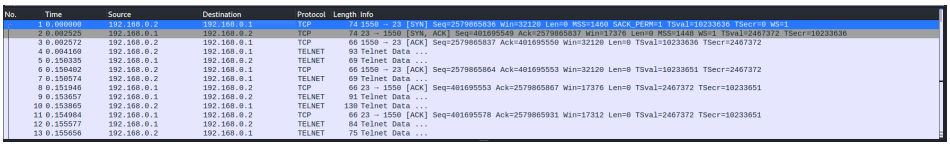
در زیر تعدادی از عکس‌های دانلود شده از سرور که توسط وایرشارک بازیابی شده‌اند را مشاهده می‌کنید.



شکل ۸: عکس‌های دانلود شده از سرور

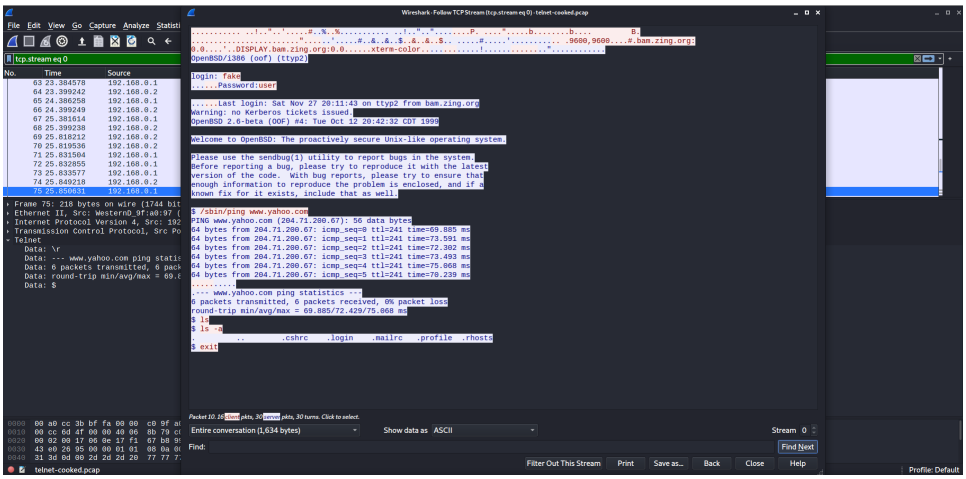
۲ سوالات بخش دوم

۱. مطابق شکل ۹ و نحوه شروع ارسال پکت‌ها و دریافت آنان، آی‌پی مربوط به کلاینت **192.168.0.2** و آی‌پی مربوط به سرور **192.168.0.1** است.



شکل ۹: وضعیت کلی پکت‌های ارسالی **Telnet**

برای دو قسمت بعدی، پکت‌های نوع **TELNET** را فیلتر کرده، روی اولین مورد کلیک راست کرده و Follow و TCP Stream را انتخاب می‌کنیم. بدین ترتیب کل دستورات و اطلاعات رد و بدل شده را مطابق شکل ۱۰ مشاهده خواهیم کرد.



شکل ۱۰: اطلاعات رد و بدل شده در **Telnet**

۲. مطابق شکل ۱۰ اطلاعات استفاده شده به صورت

```
login: fake
Password: user
```

است، پس پسورد استفاده شده **user** است.

۳. مطابق شکل ۱۰ دستورات استفاده شده چهار مورد زیر هستند:

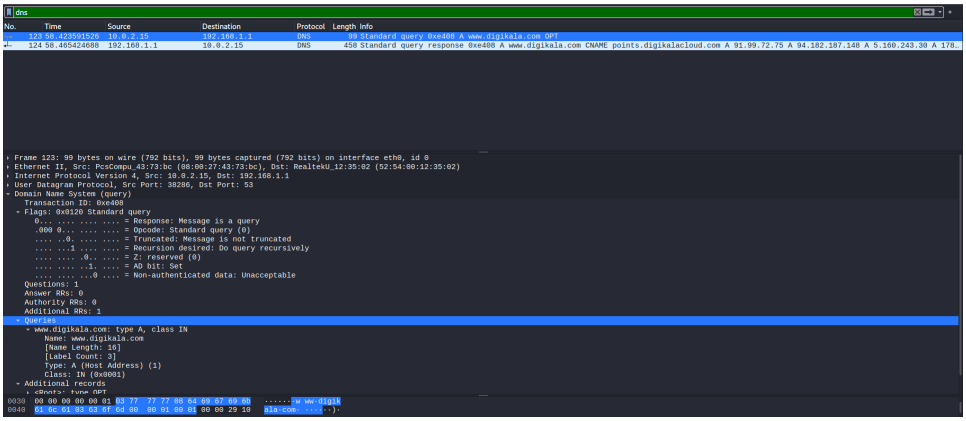
```
$ /sbin/ping www.yahoo.com
$ ls
$ ls -a
$ exit
```

۳ سوالات بخش سوم

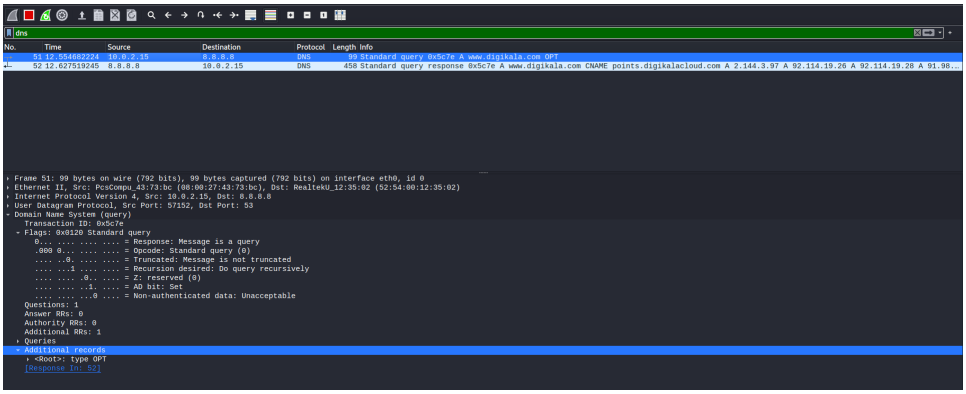
۱. مطابق شکل ۱۱ دستور را در یک سیستم‌عامل لینوکسی و برای سایت **www.digikala.com** انجام داده‌ایم. از آن جایی که فایل **/etc/resolv.conf** سیستم ما به صورت

```
nameserver 192.168.1.1
```

تنظیم شده بود، این کوئری برای **DNS** سرور لوکال یعنی **192.168.1.1** ارسال شده است. در صورتی که دستور را به صورت **dig @8.8.8.8 www.digikala.com** اجرا کنیم، دستور برای DNS Server های گوگل به آدرس **8.8.8.8** ارسال می‌شود که این موضوع را در شکل ۱۲ مشاهده می‌کنید.



شکل ۱۱: کوئری **DNS** اجرا شده از طریق دستور **dig www.digikala.com**



شکل ۱۲: کوئری **DNS** اجرا شده از طریق دستور **dig @8.8.8.8 www.digikala.com**

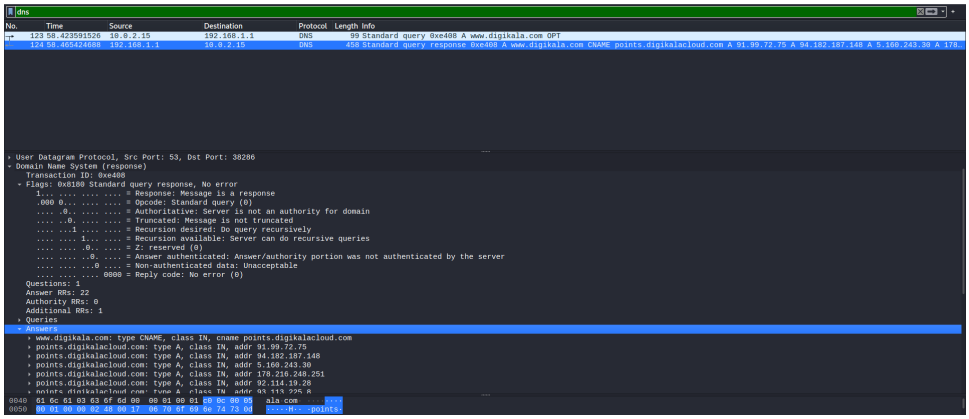
۲. مطابق شکل‌های ۱۱ و ۱۳ که به ترتیب نشان دهنده درخواست و پاسخ هستند، مشاهده می‌کنیم که همان طور که انتظار می‌رود **DNS** بر بستر **UDP** ارسال شده و سرآیندهای رایج آن نظیر پورت مبدا و مقصد را دارد.

علاوه بر آن خود **DNS** سرآیندهای مخصوص خود را هم دارد. به طور کلی کوئری و پاسخ **DNS** شامل سرآیندهای زیر است:

Identification، **Flags**، **Number of questions**، **Number of answers**، **Number of authority resource records (RRs)** و **Number of additional RR** است. در این میان تنها **flag** نیاز به توضیح اضافی دارد.

در درخواست یعنی شکل ۱۱ مشاهده می‌کنیم که فلگ مربوط به درخواست بودن ست شده است. همچنین مشخص شده که این کوئری استاندارد است. بریده (Truncate) نشده است. انجام کوئری به صورت بازگشتی مدنظر است. فلگ **AD** به معنی Authenticate Data ست شده است و در فلگ بعدی مشخص شده است که داده‌ای که Authenticate نشده قابل قبول نیست. در مورد Authenticate Data در rfc3655 توضیحاتی داده شده است.

در پاسخ یعنی شکل ۱۳ در ابتدا مشخص شده که این یک پاسخ است. سپس مشخص شده که از نوع پاسخ استاندارد است. سپس مشخص شده که سرور گفته شده یک Authoritative Server نیست. پیام بریده نشده است. انجام کوئری به صورت بازگشتی مد نظر قرار گرفته است و امکان پذیر هم بوده است. پاسخ Authenticate نشده. پاسخ Authenticate نشده قابل قبول نیست و در نهایت با کد داده شده مشخص شده که پاسخ به اروری برخورد نکرده است.



شکل ۱۳: پاسخ دریافت شده **DNS** از طریق دستور **dig www.digikala.com**