



دانشکده مهندسی کامپیوتر

سیدابوالفضل رحیمی

۹۷۱۰۵۹۴۱

پارسا ریسی

۹۸۱۰۳۲۲۳

آز شبکه

نیم سال اول ۰۲-۰۱

مدرس: دکتر صفائی

عماد زین اوقلی

۹۸۱۰۳۲۶۷

HTTP ۱

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

No.	Time	Source	Destination	Protocol	Length	Info
67	1.235217	192.168.1.4	81.31.168.10	HTTP	531	GET / HTTP/1.1
86	2.544131	81.31.168.10	192.168.1.4	HTTP	217	HTTP/1.1 200 OK (text/html)
88	2.609321	192.168.1.4	81.31.168.10	HTTP	475	GET /wp-includes/css/dist/block-library/style.min.css?ver=6.0.3 HTTP/1.1
90	2.609928	192.168.1.4	81.31.168.10	HTTP	516	GET /wp-content/plugins/social-icons-widget-by-upzoom/block/dist/style-upzoom-social-icons.css?ver=4.2.4 HTTP/1.1
101	2.641959	192.168.1.4	81.31.168.10	HTTP	482	GET /wp-content/plugins/advanced-post-slider/adps-style.css?ver=6.0.3 HTTP/1.1
105	2.646091	192.168.1.4	81.31.168.10	HTTP	467	GET /wp-content/plugins/parsi-font/assets/css/fonts.css HTTP/1.1
108	2.647651	192.168.1.4	81.31.168.10	HTTP	500	GET /wp-content/plugins/podamibe-simple-footer-widget-area/assets/css/sfwa.css?ver=2.0.8 HTTP/1.1
115	2.652157	192.168.1.4	81.31.168.10	HTTP	504	GET /wp-content/plugins/responsive-header-image-slider/css/responsiveimgslider.css?ver=3.0.3 HTTP/1.1
127	2.662953	81.31.168.10	192.168.1.4	HTTP	639	HTTP/1.1 200 OK (text/css)
129	2.662953	81.31.168.10	192.168.1.4	HTTP	873	HTTP/1.1 200 OK (text/css)
132	2.663828	192.168.1.4	81.31.168.10	HTTP	496	GET /wp-content/plugins/events-manager/includes/css/events-manager.min.css?ver=6.1.3 HTTP/1.1
133	2.664467	192.168.1.4	81.31.168.10	HTTP	464	GET /wp-content/themes/academica/style.css?ver=6.0.3 HTTP/1.1
141	2.683767	192.168.1.4	81.31.168.10	HTTP	470	GET /wp-content/themes/academica/media-queries.css?ver=1.0 HTTP/1.1
143	2.686454	81.31.168.10	192.168.1.4	HTTP	1333	HTTP/1.1 200 OK (text/css)
145	2.687085	192.168.1.4	81.31.168.10	HTTP	460	GET /wp-includes/css/dashicons.min.css?ver=6.0.3 HTTP/1.1
148	2.695772	81.31.168.10	192.168.1.4	HTTP	1109	HTTP/1.1 200 OK (text/css)
150	2.696367	192.168.1.4	81.31.168.10	HTTP	510	GET /wp-content/plugins/social-icons-widget-by-upzoom/assets/css/upzoom-social-icons.css?ver=1650425856 HTTP/1.1
155	2.714294	81.31.168.10	192.168.1.4	HTTP	1186	HTTP/1.1 200 OK (text/css)
157	2.714853	192.168.1.4	81.31.168.10	HTTP	506	GET /wp-content/plugins/social-icons-widget-by-upzoom/assets/css/genericons.css?ver=1650425856 HTTP/1.1
216	2.853225	81.31.168.10	192.168.1.4	HTTP	785	HTTP/1.1 200 OK (text/css)
219	2.854041	192.168.1.4	81.31.168.10	HTTP	513	GET /wp-content/plugins/social-icons-widget-by-upzoom/assets/css/academicons.min.css?ver=1650425856 HTTP/1.1
222	2.858956	81.31.168.10	192.168.1.4	HTTP	623	HTTP/1.1 200 OK (text/css)
229	2.859682	192.168.1.4	81.31.168.10	HTTP	514	GET /wp-content/plugins/social-icons-widget-by-upzoom/assets/css/font-awesome-3.min.css?ver=1650425856 HTTP/1.1
240	2.871808	192.168.1.4	81.31.168.10	HTTP	522	GET /wp-content/plugins/social-icons-widget-by-upzoom/assets/css/upzoom-social-icons-styles.css?ver=1650425856 HTTP/1.1
277	2.897773	81.31.168.10	192.168.1.4	HTTP	1177	HTTP/1.1 200 OK (text/css)
278	2.897773	81.31.168.10	192.168.1.4	HTTP	490	HTTP/1.1 200 OK (text/css)
283	2.899792	192.168.1.4	81.31.168.10	HTTP	517	GET /wp-content/plugins/social-icons-widget-by-upzoom/assets/font/academicons.ttf?ver=1.8.6 HTTP/1.1

شکل ۱: فیلتر بر حسب پروتکل HTTP

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

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	2572	100.0	1945568	2334 k	0	0	0	2572
Ethernet	100.0	2572	1.9	36008	43 k	0	0	0	2572
Internet Protocol Version 4	99.9	2570	2.6	51400	61 k	0	0	0	2570
User Datagram Protocol	3.7	94	0.0	752	902	0	0	0	94
QUIC IETF	0.6	16	1.0	20000	23 k	16	20000	23 k	16
Domain Name System	3.0	78	0.2	3287	3943	78	3287	3943	78
Transmission Control Protocol	96.3	2476	94.3	1834065	2200 k	1801	1055581	1266 k	2476
Transport Layer Security	4.9	127	4.8	93172	111 k	127	87581	105 k	128
Hypertext Transfer Protocol	21.3	548	51.0	992527	1190 k	512	652339	782 k	548
Portable Network Graphics	0.1	2	0.2	3091	3708	2	3091	3708	2
Media Type	0.6	15	12.6	246058	295 k	15	246058	295 k	15
Line-based text data	0.5	14	28.8	559770	671 k	14	559770	671 k	14
JPEG File Interchange Format	0.2	4	4.8	93317	111 k	4	93317	111 k	4
CompuServe GIF	0.0	1	0.4	8581	10 k	1	8581	10 k	1
Address Resolution Protocol	0.1	2	0.0	56	67	2	56	67	2

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.

Transmission Control Protocol, Src Port: 22871, Dst Port: 80, Seq: 606236787, Ack: 95071967, Len: 477
 Source Port: 22871
 Destination Port: 80
 [Stream index: 9]
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 477]
 Sequence Number: 606236787
 [Next Sequence Number: 606237264]
 Acknowledgment Number: 95071967
 0101 = Header Length: 20 bytes (5)

شکل ۳: اولین درخواست TCP

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

No.	dns	Source	Destination	Protocol	Length	Info
116	192.168.1.4	85.15.1.14	DNS	74	Standard query 0xa2bd A math.sharif.ir	
17 0.945680	192.168.1.4	85.15.1.15	DNS	74	Standard query 0xa2bd A math.sharif.ir	
55 1.208474	85.15.1.14	192.168.1.4	DNS	90	Standard query response 0xa2bd A math.sharif.ir A 81.31.168.10	
68 1.268710	85.15.1.15	192.168.1.4	DNS	90	Standard query response 0xa2bd A math.sharif.ir A 81.31.168.10	
94 2.614650	192.168.1.4	85.15.1.14	DNS	83	Standard query 0x6d9a A maxcdn.bootstrapcdn.com	
112 2.651848	85.15.1.14	192.168.1.4	DNS	115	Standard query response 0x6d9a A maxcdn.bootstrapcdn.com A 104.18.10.207 A 104.18.11.207	
176 2.815573	192.168.1.4	85.15.1.14	DNS	80	Standard query 0xc682 A fonts.googleapis.com	
204 2.844283	192.168.1.4	85.15.1.14	DNS	67	Standard query 0xc682 A s.w.org	
220 2.856101	192.168.1.4	85.15.1.15	DNS	80	Standard query 0xc682 A fonts.googleapis.com	
254 2.887356	192.168.1.4	85.15.1.15	DNS	67	Standard query 0xc682 A s.w.org	
266 2.896385	85.15.1.14	192.168.1.4	DNS	90	Standard query response 0xc682 A fonts.googleapis.com A 172.217.21.170	
279 2.897773	85.15.1.14	192.168.1.4	DNS	83	Standard query response 0xc682 A s.w.org A 192.0.77.48	
385 3.009620	85.15.1.15	192.168.1.4	DNS	90	Standard query response 0xc682 A fonts.googleapis.com A 142.250.184.234	
420 3.027610	85.15.1.15	192.168.1.4	DNS	83	Standard query response 0xc682 A s.w.org A 192.0.77.48	
1227 3.091983	192.168.1.4	85.15.1.14	DNS	77	Standard query 0xb058 A fonts.gstatic.com	
1267 3.123261	192.168.1.4	85.15.1.15	DNS	77	Standard query 0xb058 A fonts.gstatic.com	
1293 3.150812	85.15.1.14	192.168.1.4	DNS	93	Standard query response 0xb058 A fonts.gstatic.com A 142.250.74.35	
1317 3.190879	85.15.1.15	192.168.1.4	DNS	93	Standard query response 0xb058 A fonts.gstatic.com A 142.250.185.67	
1510 4.107911	192.168.1.4	85.15.1.14	DNS	72	Standard query 0xb088f A frontiers.ir	
1511 4.107957	192.168.1.4	85.15.1.14	DNS	72	Standard query 0xf199 A ia.sharif.ir	
1512 4.111837	192.168.1.4	85.15.1.14	DNS	84	Standard query 0xb56b A calculus.math.sharif.edu	
1530 4.150902	192.168.1.4	85.15.1.15	DNS	72	Standard query 0xb088f A frontiers.ir	
1531 4.150994	192.168.1.4	85.15.1.15	DNS	72	Standard query 0xf199 A ia.sharif.ir	
1532 4.151076	192.168.1.4	85.15.1.15	DNS	84	Standard query 0xb56b A calculus.math.sharif.edu	
1625 4.227892	85.15.1.14	192.168.1.4	DNS	88	Standard query response 0xb088f A frontiers.ir A 194.225.73.180	
1674 4.261346	85.15.1.14	192.168.1.4	DNS	127	Standard query response 0xb56b A calculus.math.sharif.edu CNAME webhosting01.sharif.edu A 81.31.168.10	
1676 4.262640	192.168.1.4	85.15.1.14	DNS	70	Standard query 0xb048 A en.isti.ir	
1677 4.262640	192.168.1.4	85.15.1.14	DNS	69	Standard query 0xc241 A en.bmn.ir	
1726 4.306667	192.168.1.4	85.15.1.15	DNS	69	Standard query 0xc241 A en.bmn.ir	
1727 4.306667	192.168.1.4	85.15.1.15	DNS	70	Standard query 0xb048 A en.isti.ir	
1743 4.314788	85.15.1.15	192.168.1.4	DNS	88	Standard query response 0xb088f A frontiers.ir A 194.225.73.180	
1747 4.314788	85.15.1.15	192.168.1.4	DNS	88	Standard query response 0xf199 A ia.sharif.ir A 10.10.34.35	
1752 4.316658	192.168.1.4	85.15.1.14	DNS	60	Standard query 0xc321d A ipw.ir	
1759 4.319173	85.15.1.15	192.168.1.4	DNS	127	Standard query response 0xb56b A calculus.math.sharif.edu CNAME webhosting01.sharif.edu A 81.31.168.10	
1808 4.352405	192.168.1.4	85.15.1.15	DNS	66	Standard query 0xc321d A ipw.ir	
1908 4.429324	85.15.1.14	192.168.1.4	DNS	80	Standard query response 0xb048 A en.isti.ir A 194.225.136.49	
1909 4.429324	85.15.1.14	192.168.1.4	DNS	85	Standard query response 0xc241 A en.bmn.ir A 46.209.44.178	

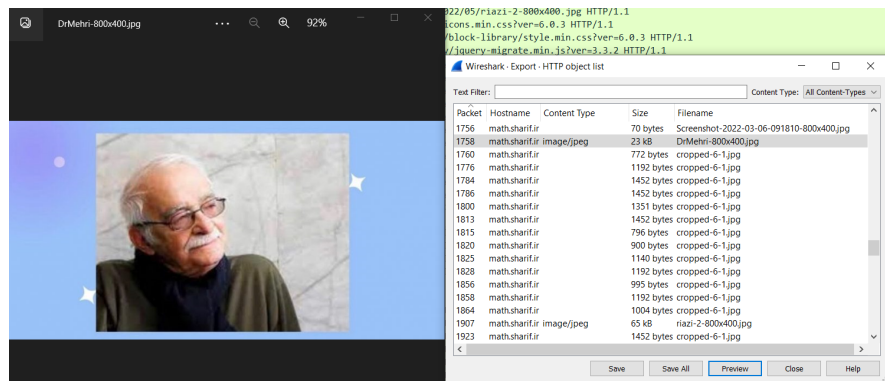
شکل ۴: فیلتر بر حسب پروتکل DNS

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

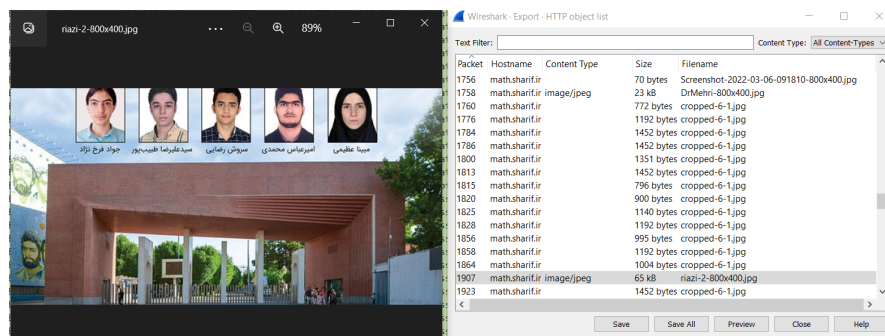
The screenshot shows the Wireshark application window. The 'File' menu is open, and the 'Export Objects' option is selected. A sub-menu is displayed with 'HTTP...' highlighted. The packet list on the right shows several HTTP packets from 192.168.1.4 to 81.31.168.10.

شکل ۵: HTTP: Export Objects

دو نمونه زیر را انتخاب کردیم.



شکل ۶: نمونه اول



شکل ۷: نمونه دوم

Telnet ۲

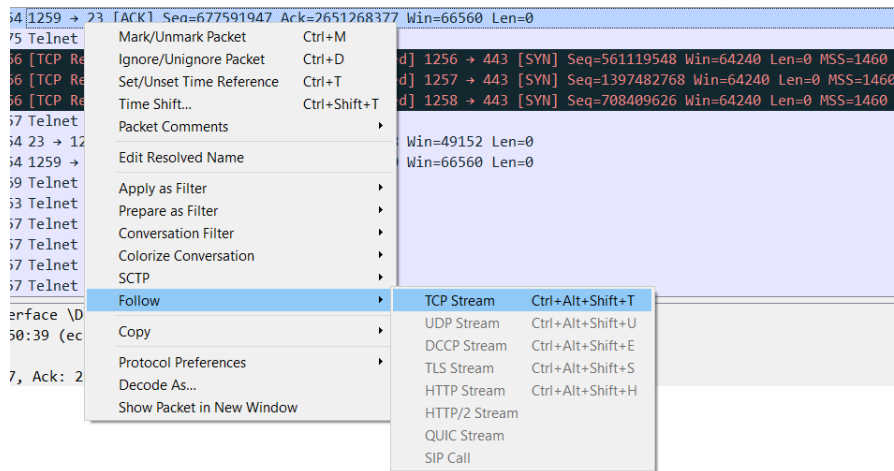
۱. با توجه به جواب DNS می فهمیم که IP آدرس سرور 230.139.13.64 و آدرس کلاینت 4.1.168.192 است.

88	3.637444	85.15.1.14	192.168.1.4	DNS	88 Standard query response 0x8e50 A telehack.com A 64.13.139.230
89	3.637444	85.15.1.14	192.168.1.4	DNS	88 Standard query response 0x8e50 A telehack.com A 64.13.139.230
90	3.639462	192.168.1.4	64.13.139.230	TCP	66 1259 → 23 [SYN] Seq=677591946 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
91	3.716853	85.15.1.15	192.168.1.4	DNS	88 Standard query response 0x8e50 A telehack.com A 64.13.139.230
92	3.964926	64.13.139.230	192.168.1.4	TCP	66 23 → 1259 [SYN, ACK] Seq=2651268376 Ack=677591947 Win=42340 Len=0 MSS=145
93	3.964991	192.168.1.4	64.13.139.230	TCP	54 1259 → 23 [ACK] Seq=677591947 Ack=2651268377 Win=66560 Len=0
94	3.965442	192.168.1.4	64.13.139.230	TELNET	75 Telnet Data ...
95	4.013441	192.168.1.4	107.187.124.2	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 1256 → 443 [SYN] Seq=56111
96	4.013442	192.168.1.4	89.252.132.35	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 1257 → 443 [SYN] Seq=13974
97	4.013512	192.168.1.4	89.252.132.19	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 1258 → 443 [SYN] Seq=78848
98	4.270753	64.13.139.230	192.168.1.4	TELNET	57 Telnet Data ...
99	4.274053	64.13.139.230	192.168.1.4	TCP	54 23 → 1259 [ACK] Seq=2651268380 Ack=677591968 Win=49152 Len=0
100	4.315559	192.168.1.4	64.13.139.230	TCP	54 1259 → 23 [ACK] Seq=677591968 Ack=2651268380 Win=66560 Len=0
101	4.605495	64.13.139.230	192.168.1.4	TELNET	1269 Telnet Data ...
102	4.605705	192.168.1.4	64.13.139.230	TELNET	63 Telnet Data ...
103	4.605777	192.168.1.4	64.13.139.230	TELNET	57 Telnet Data ...
104	4.605829	192.168.1.4	64.13.139.230	TELNET	57 Telnet Data ...
105	4.605864	192.168.1.4	64.13.139.230	TELNET	57 Telnet Data ...
106	4.605894	192.168.1.4	64.13.139.230	TELNET	57 Telnet Data ...

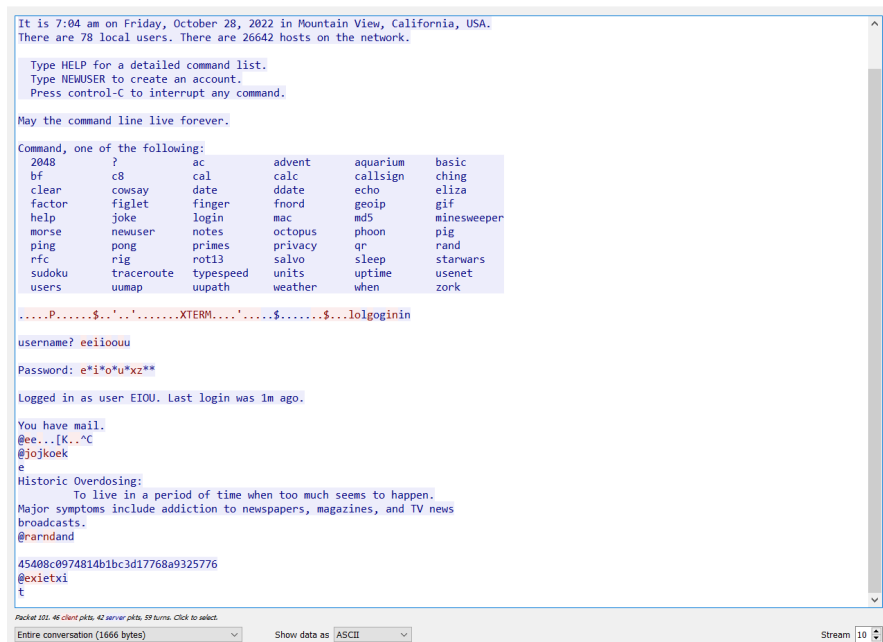
> Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > telehack.com: type A, class IN
 > Answers
 > telehack.com: type A, class IN, addr 64.13.139.230
 [Request In: 9]
 [Time: 1.647707000 seconds]

شکل ۸: IP Address

۲. با استفاده از قابلیت Follow TCP Stream ۹ می توان 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	2.639994	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 nsl.sharif.ir

شکل ۱۲: فیلتر برحسب DNS

۱. با توجه به ۱۱ و ۱۲ در می‌یابیم که درخواست‌ها به و پاسخ‌ها از سرور 85.15.1.14 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)
... .. = 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.

```

Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... 0... .. = Authoritative: Server is not an authority for domain
... 0... .. = Truncated: Message is not truncated
... 1... .. = Recursion desired: Do query recursively
... 1... .. = Recursion available: Server can do recursive queries
... 0... .. = Z: reserved (0)
... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
... 0... .. = Non-authenticated data: Unacceptable
... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
> sharif.ir: type A, class IN
Answers
> sharif.ir: type A, class IN, addr 152.89.13.54
[Request In: 5]
[Time: 0.297261000 seconds]

```

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 54.13.89.152 است.