



دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

گزارش آزمایش دوم

عنوان آزمایش : آشنایی با نرم افزار wireshark

دکتر بردیا صفایی

سارا آذرنوش — ۹۸۱۷۰۶۶۸

کهد آئینی — ۹۸۱۰۱۲۰۹

پارسا محمدیان — ۹۸۱۰۲۲۸۴

۱۶ اسفند ۱۴۰۲

فهرست مطالب

۲	بخش اول (فهم اولیه از HTTP)	۱
۲	۱.۱	
۲	۲.۱	
۲	۳.۱	
۴	۴.۱	
۴	بخش دوم (بررسی ارتباط از طریق Telnet)	۲
۴	۱.۲	
۴	۲.۲	
۷	۳.۲	
۱۰	بخش سوم (بررسی درخواست‌ها و پاسخ‌های DNS)	۳
۱۰	۱.۳	
۱۲	۲.۳	

Wireshark - Protocol Hierarchy Statistics - wlp3s0

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	1993	100.0	1746271	5,650 k	0	0	0	1993
Ethernet	100.0	1993	1.6	27902	90 k	0	0	0	1993
Internet Protocol Version 4	100.0	1993	2.3	39860	128 k	0	0	0	1993
User Datagram Protocol	0.9	18	0.0	144	465	0	0	0	18
Domain Name System	0.4	8	0.0	410	1,326	8	410	1,326	8
Data	0.5	10	0.2	3548	11 k	10	3548	11 k	10
Transmission Control Protocol	99.0	1974	95.9	1674407	5,417 k	1857	1535422	4,967 k	1974
Transport Layer Security	3.4	68	4.4	77320	250 k	68	77320	250 k	68
SSH Protocol	0.1	2	0.0	152	491	2	152	491	2
Hypertext Transfer Protocol	2.4	47	3.6	62056	200 k	42	48539	157 k	47
Media Type	0.1	1	0.0	738	2,387	1	738	2,387	1
Malformed Packet	0.1	2	0.0	0	0	2	0	0	2
Line-based text data	0.1	2	0.2	3431	11 k	2	3431	11 k	2
Data	0.1	1	0.1	1480	4,788	1	1480	4,788	1

No display filter.

Help Copy Close

شکل ۱: آمار پروتکل‌های استفاده شده

۱ بخش اول (فهم اولیه از HTTP)

برای این بخش، از آنجایی که نیاز به بررسی پروتکل HTTP داشتیم، نمیتوانستیم از آدرس گفته شده در دستور کار (<https://sharif.edu>) که بر بستر HTTPS است استفاده کنیم. به همین دلیل از صفحه <http://sharif.edu/~asadi/> که بر بستر HTTP است، استفاده کردیم.

۱.۱

برای تجمیع پیام‌های مربوط به هر پروتکل، از گزینه Statistics و سپس Protocol Hierarchy استفاده می‌کنیم. تصویر مربوط به این بخش در شکل ۱ قابل مشاهده است. طبق این آمار، در کل ۱۹۹۳ بسته منتقل شده است که ۱۸ عدد مربوط به پروتکل UDP و ۱۹۷۴ عدد مربوط به پروتکل TCP بوده است. از بین بسته‌های مربوط به TCP نیز ۴۷ عدد مربوط به HTTP بوده است. تعداد بسته‌های بقیه پروتکل‌ها در شکل قابل مشاهده است. همچنین حجم عمده پیام‌های رد و بدل شده مربوط به پروتکل TCP است.

۲.۱

همانطور که در شکل ۲ مشخص است، اختلاف زمانی بین اولین درخواست GET و اولین جواب OK بسیار کم و حدود ۶۷ هزارم است. اگر اولین درخواست TCP را بررسی کنیم، طبق انتظار شماره ترتیب نسبی آن ۱ است. با توجه به شکل ۳ شماره ترتیب مطلق آن ۴۰۰۴۸۵۵۲۹۸ است.

۳.۱

همانطور که در شکل ۴ مشاهده می‌کنیم، برای دریافت آدرس آی‌پی دامنه sharif.edu درخواست‌های DNS متعددی فرستاده شده. این به دلیل معماری سلسله مراتبی DNS است. این کوئری‌های انواع مختلفی اعم از A، CNAME، AAAA دارند.

No.	Time	Source	Destination	Protocol	Length	Info
821	12.304697469	192.168.100.48	152.89.13.54	HTTP	500	GET /favicon.ico HTTP/1.1
823	12.309395506	152.89.13.54	192.168.100.48	HTTP	548	HTTP/1.1 404 Not Found (text/css)
995	16.235504690	192.168.100.48	152.89.13.54	HTTP	604	GET /~asadi/ HTTP/1.1
1013	16.258579221	192.168.100.48	152.89.13.54	HTTP	531	GET /~asadi/vendor/bootstrap
1057	16.285889960	192.168.100.48	152.89.13.54	HTTP	532	GET /~asadi/vendor/fontawesome
1058	16.285905349	192.168.100.48	152.89.13.54	HTTP	511	GET /~asadi/css/resume.min.css
1090	16.292870107	192.168.100.48	152.89.13.54	HTTP	554	GET /~asadi/img/profile.jpg
1104	16.302698032	152.89.13.54	192.168.100.48	HTTP	1431	HTTP/1.1 200 OK (text/html)
1107	16.303812769	192.168.100.48	152.89.13.54	HTTP	505	GET /~asadi/vendor/jquery/jquery
1145	16.338200493	152.89.13.54	192.168.100.48	HTTP	2229	HTTP/1.1 200 OK (text/css)
1149	16.338711491	192.168.100.48	152.89.13.54	HTTP	521	GET /~asadi/vendor/bootstrap
1191	16.357053751	192.168.100.48	152.89.13.54	HTTP	519	GET /~asadi/vendor/jquery-ea
1407	16.441033108	152.89.13.54	192.168.100.48	HTTP	1553	HTTP/1.1 200 OK (application/javascript)
1412	16.442732300	192.168.100.48	152.89.13.54	HTTP	494	GET /~asadi/js/resume.min.js

شکل ۲: فاصله زمانی بین درخواست GET و OK

Wireshark - Packet 821 - wlp3s0

- Frame 821: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits) on interface wlp3s0, id 0
- Ethernet II, Src: AzureWav_c2:68:55 (d0:c5:d3:c2:68:55), Dst: 12:c4:d4:27:4d:d8 (12:c4:d4:27:4d:d8)
- Internet Protocol Version 4, Src: 192.168.100.48, Dst: 152.89.13.54
- Transmission Control Protocol, Src Port: 38012, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
 - Source Port: 38012
 - Destination Port: 80
 - [Stream index: 48]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 434]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 4004855298
 - [Next Sequence Number: 435 (relative sequence number)]
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 2369752930
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x018 (PSH, ACK)
 - Window: 502
 - [Calculated window size: 64256]

No.: 821 · Time: 12.304697469 · Source: 192.168.100.48 · Destination: 152.89.13.54 · Protocol: HTTP · Length: 500 · Info: GET /favicon.ico HTTP/1.1

☐ Show packet bytes

Help Close

شکل ۳: اولین ارتباط TCP

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
*wip3d0

🔍 📄 📊 📌 📁 📂 📅

No.	Time	Source	Destination	Protocol	Length	Info
28	0.743092452	192.168.100.48	200.07.222.222	UDP	72	Standard query 0x0040 A C0-sharif1.600
29	0.743099432	192.168.100.48	200.07.222.222	UDP	72	Standard query 0x0040 A C0-sharif1.600
30	1.130026822	200.07.222.222	192.168.100.48	UDP	89	Standard query response 0x0040 A C0-sharif1.600 A 192.09.13.27
31	1.476707680	192.168.100.48	200.07.222.222	UDP	77	Standard query 0x0070 A 00n-C0-sharif1.600
32	1.476708426	192.168.100.48	200.07.222.222	UDP	77	Standard query 0x0070 AAAA 00n-C0-sharif1.600
33	1.584200000	200.07.222.222	192.168.100.48	UDP	132	Standard query response 0x0040 AAAA C0-sharif1.600 S0A 00n-sharif1.37
34	1.584200822	192.168.100.48	200.07.222.222	UDP	72	Standard query 0x0070 A 00n-sharif1.37
35	1.584200874	192.168.100.48	200.07.222.222	UDP	72	Standard query 0x0070 AAAA 00n-sharif1.37
36	1.780057242	192.168.100.48	200.07.222.222	UDP	72	Standard query 0x0040 A 10c-sharif1.37
37	1.780058000	192.168.100.48	200.07.222.222	UDP	72	Standard query 0x0040 AAAA 10c-sharif1.37
38	1.974717676	200.07.222.222	192.168.100.48	UDP	111	Standard query response 0x0070 A 00n-sharif1.37 CNAME 00n-10c-sharif1.37 A 01.31.178.00
39	1.984456330	200.07.222.222	192.168.100.48	UDP	104	Standard query response 0x0040 AAAA 10c-sharif1.37 S0A 00n-sharif1.37
40	1.984456997	200.07.222.222	192.168.100.48	UDP	104	Standard query response 0x0040 A 10c-sharif1.37 S0A 00n-sharif1.37
41	2.004767274	200.07.222.222	192.168.100.48	UDP	137	Standard query response 0x0070 AAAA 00n-C0-sharif1.600 S0A 00n-sharif1.37
42	2.004767298	200.07.222.222	192.168.100.48	UDP	146	Standard query response 0x0070 AAAA 00n-sharif1.37 CNAME 00n-10c-sharif1.37 S0A 00n-sharif1.37
43	2.004771258	200.07.222.222	192.168.100.48	UDP	93	Standard query response 0x0070 A 00n-C0-sharif1.600 A 01.31.100.100
44	2.409829887	192.168.100.48	200.07.222.222	UDP	77	Standard query 0x0070 A 00n-00-sharif1.600
45	2.409829894	192.168.100.48	200.07.222.222	UDP	77	Standard query 0x0070 AAAA 00n-00-sharif1.600
46	2.700774444	200.07.222.222	192.168.100.48	UDP	111	Standard query response 0x0040 A 00n-00-sharif1.600 CNAME 00n-sharif1.600 A 192.09.13.27
47	2.700780091	200.07.222.222	192.168.100.48	UDP	105	Standard query response 0x0040 AAAA 00n-00-sharif1.600 CNAME 00n-sharif1.600 S0A 00n-sharif1.37

wireshark_wip3d0LPHC11.pcapng
Packets: 174 · Displayed: 20 (11.5%) · Dropped: 0 (0.0%)
Profile: Default

شکل ۴: درخواست‌های DNS

۲.۱

همانطور که شکل ۵ مشاهده می‌کنیم، یک ریکوئست مربوط به عکس ارسال شده که پاسخ آن هم در ادامه آماده است.

برای بازیابی عکس‌های که در صفحه موجود هستند، گزینه File، Export Objects، HTTP... را انتخاب می‌کنیم. سپس از صفحه‌ی جدید عکس مورد نظر خود را انتخاب می‌کنیم و مسیر ذخیره آن را وارد می‌کنیم. نتیجه انجام این مراحل در شکل ۶ نشان داده شده است.

۲ بخش دوم (بررسی ارتباط از طریق Telnet)

در شکل ۷ به آدرس مورد نظر وصل شده‌ام و دستور joke را اجرا کرده‌ام. همانطور که در نرم‌افزار Wirehark مشخص است، خروجی این دستور به صورت plain text ارسال شده و به راحتی قابل خواندن توسط فرد مهاجم و شنود کننده است.

1.2

ابتدا بسته‌ها را بر اساس پروتکل ارتباطی Telnet فیلتر می‌کنیم. سپس مشاهده می‌کنیم که مبدا و مقصد تمامی بسته‌ها آی‌پی‌های 192.168.0.1 و 192.168.0.2 هستند. با بررسی متن برخی از پیام‌ها (برای مثال پیامی که در شکل ۸ مشاهده می‌شود) متوجه می‌شویم که آی‌پی اول سرور، و آی‌پی دوم کلاینت است.

۲.۲

در بسته‌ای که در شکل ۹ آمده، مشاهده می‌کنیم سرور درخواست پسورد را از کلاینت کرده است. البته توجه شود که قبل از آن کلاینت خود درخواست login داده است. انتظار داریم که در بسته بعدی کلاینت

Wireshark interface showing a list of captured packets. The selected packet (No. 1098) is an HTTP GET request for /asadi/img/profile.jpg.

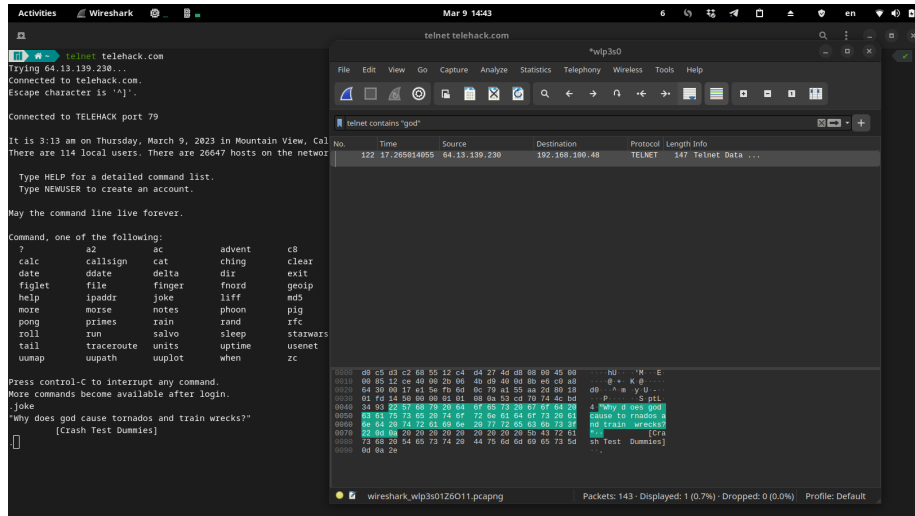
No.	Time	Source	Destination	Protocol	Length	Info
823	16.82490907405	192.168.1.100	192.168.1.1	HTTP	512	GET /favicon.ico HTTP/1.1
1104	16.8260905006	192.168.1.100	192.168.1.1	HTTP	504	GET /~asadi/ HTTP/1.1
1145	16.8263040606	192.168.1.100	192.168.1.1	HTTP	504	GET /~asadi/vendor/jquery.easing.min.js HTTP/1.1
1407	16.826517224	192.168.1.100	192.168.1.1	HTTP	504	GET /~asadi/vendor/font-awesome/css/font-awesome.min.css HTTP/1.1
1511	16.8266880606	192.168.1.100	192.168.1.1	HTTP	511	GET /~asadi/vendor/css/font-awesome.min.css HTTP/1.1
1635	16.8268003399	192.168.1.100	192.168.1.1	HTTP	511	GET /~asadi/css/font-awesome.min.css HTTP/1.1
1098	16.8292781...	192.168.1.100	192.168.1.1	HTTP	554	GET /asadi/img/profile.jpg HTTP/1.1
1105	16.8292998092	192.168.1.100	192.168.1.1	HTTP	1433	HTTP/1.1 200 OK (text/html)
1107	16.829327709	192.168.1.100	192.168.1.1	HTTP	505	GET /~asadi/vendor/jquery/jquery.min.js HTTP/1.1
1145	16.8292694092	192.168.1.100	192.168.1.1	HTTP	2229	HTTP/1.1 200 OK (text/css)
1145	16.8297114092	192.168.1.100	192.168.1.1	HTTP	521	GET /~asadi/vendor/jquery.easing.min.js HTTP/1.1
1107	16.8297114092	192.168.1.100	192.168.1.1	HTTP	519	GET /~asadi/vendor/jquery.easing.min.js HTTP/1.1
1407	16.844622408	192.168.1.100	192.168.1.1	HTTP	1053	HTTP/1.1 200 OK (application/javascript)
1412	16.842732200	192.168.1.100	192.168.1.1	HTTP	491	GET /~asadi/js/font-awesome.min.js HTTP/1.1
1414	16.8467054092	192.168.1.100	192.168.1.1	HTTP	508	Content-Disposition
1511	16.846126308	192.168.1.100	192.168.1.1	HTTP	10853	HTTP/1.1 200 OK (text/css)
1635	16.827310009	192.168.1.100	192.168.1.1	HTTP	1157	HTTP/1.1 200 OK (application/javascript)
1688	16.830112008	192.168.1.100	192.168.1.1	HTTP	508	Content-Disposition (multipart)
2912	16.824192183	192.168.1.100	192.168.1.1	HTTP	713	HTTP/1.1 200 OK (JPEG JFIF image)
3109	17.092311753	192.168.1.100	192.168.1.1	HTTP	542	GET /asadi/img/profile.jpg HTTP/1.1
3109	17.090900357	192.168.1.100	192.168.1.1	HTTP	547	HTTP/1.1 404 Not Found (text/html)

شکل ۵: درخواست و پاسخ عکس

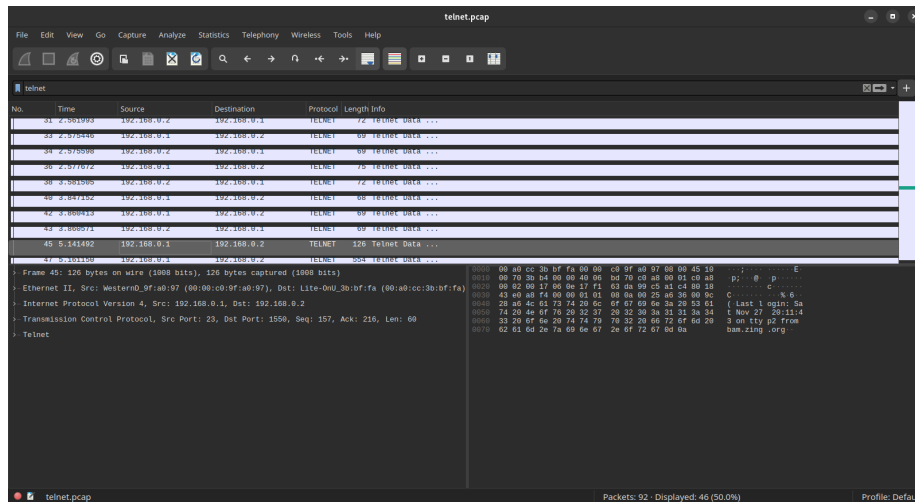
Wireshark interface showing the 'Export - HTTP object list' window. The selected object is 'profile.jpg' (1.1 MB).

Packet	Hostname	Content Type	Size	Filename
823	sharif.edu	text/html	209 bytes	favicon.ico
1104	sharif.edu	text/html	51 kB	~asadi
1145	sharif.edu	text/css	3,222 bytes	resume.min.css
1407	sharif.edu	application/javascript	2,532 bytes	jquery.easing.min.js
1511	sharif.edu	text/css	54 kB	all.min.css
1635	sharif.edu	application/javascript	738 bytes	resume.min.js
2912	sharif.edu	image/jpeg	1,062 kB	profile.jpg
3109	sharif.edu	text/html	209 bytes	favicon.ico

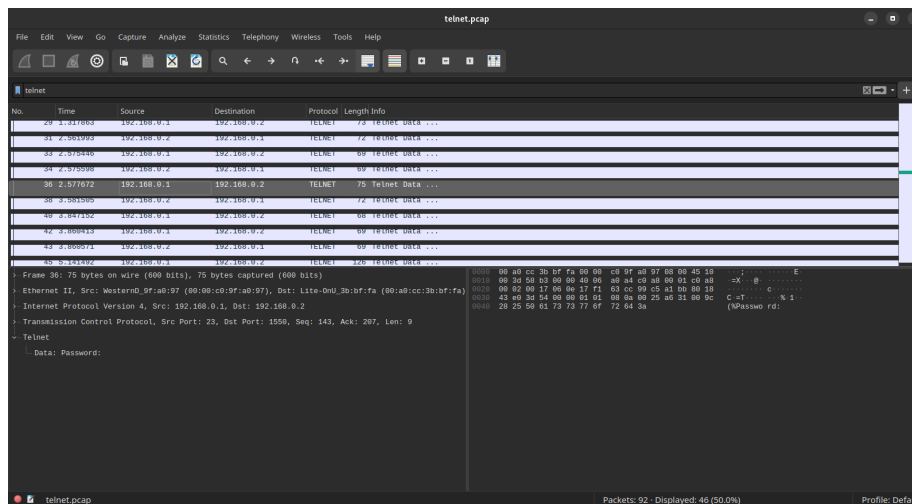
شکل ۶: بازبینی عکس موجود در صفحه وب



شکل ۷: اتصال به Telnet



شکل ۸: تشخیص کلاینت و سرور ارتباط Telnet



شکل ۹: درخواست پسورد توسط سرور Telnet

پسورد را برای سرور ارسال کند که همین اتفاق هم افتاده است. در شکل ۱۰ مشاهده میکنیم که کلاینت پسورد را برای سرور فرستاده است و پسورد برابر رشته user است.

۳.۲

برای بررسی دستورات ارسالی از طرف کلاینت، فیلتر زیر را اعمال میکنیم.

```
telnet && ip.src == 192.168.0.2
```

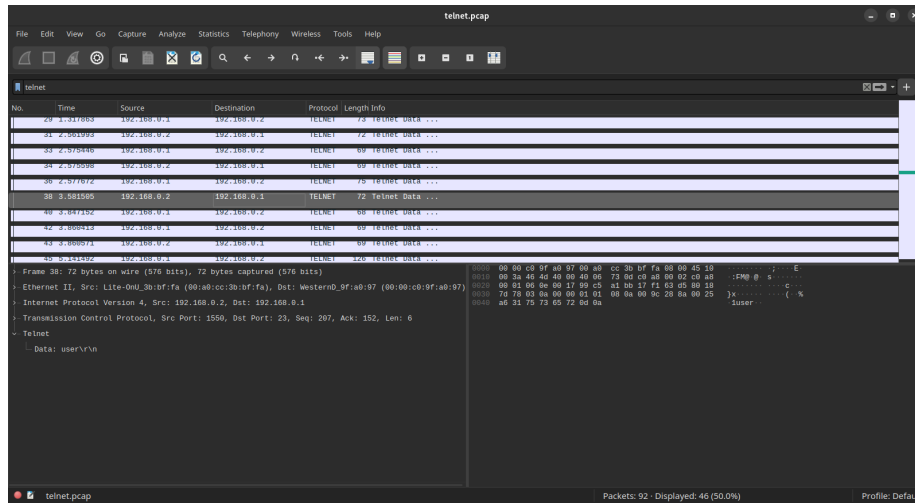
سپس پکت‌ها را برای پیدا کردن دستورات به ترتیب چک می‌کنیم. دستورات اجرا شده به ترتیب در شکل‌های ۱۱، ۱۲، ۱۳، ۱۴ قابل مشاهده هستند و در زیر شرح داده شده‌اند.

۱. `/sbin/ping www.yahoo.com` با استفاده از این دستور پینگ سرور را تا سرور سایت یاهو اندازه میگیرد.

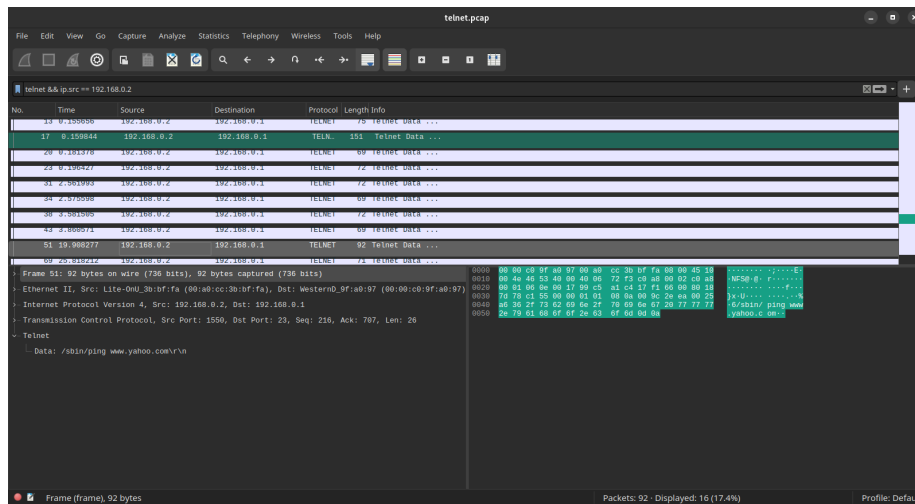
۲. `ls` با این دستور فایل‌های موجود در سرور در پوشه فعلی را لیست می‌کند.

۳. `ls -a` مانند همان دستور قبلی با این تفاوت که همه فایل‌ها (شامل آن‌هایی که هاید شده‌اند) را نشان می‌دهد.

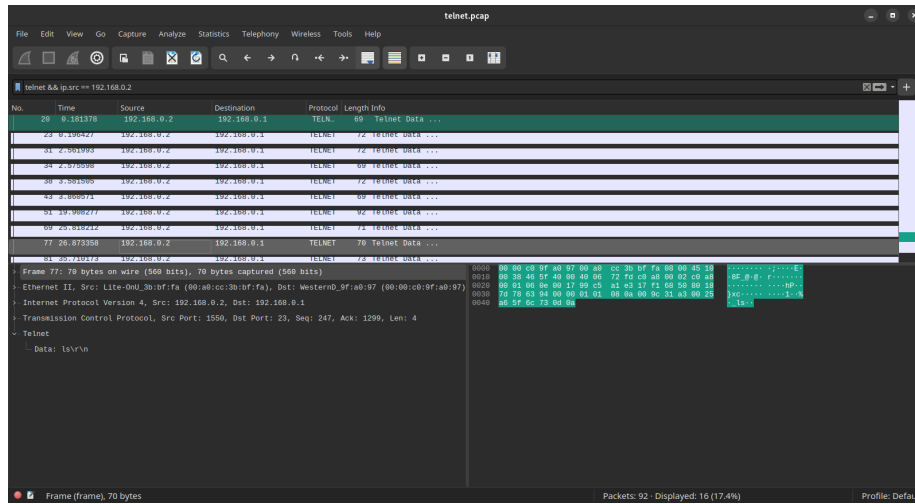
۴. `exit` از ترمینال سرور خارج می‌شود.



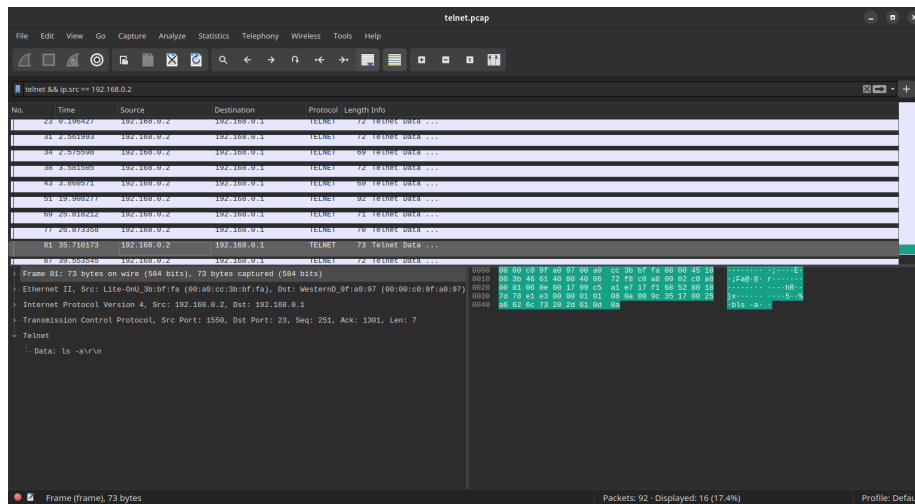
شکل ۱۰: ارسال پسورد توسط کلاینت Telnet



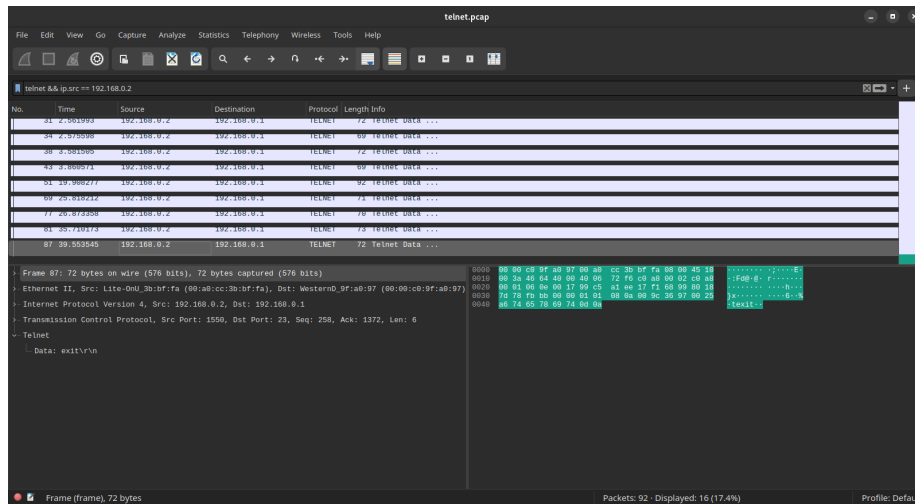
شکل ۱۱: کامند اجرا شده در Telnet



شکل ۱۲: کامند اجرا شده در Telnet



شکل ۱۳: کامند اجرا شده در Telnet

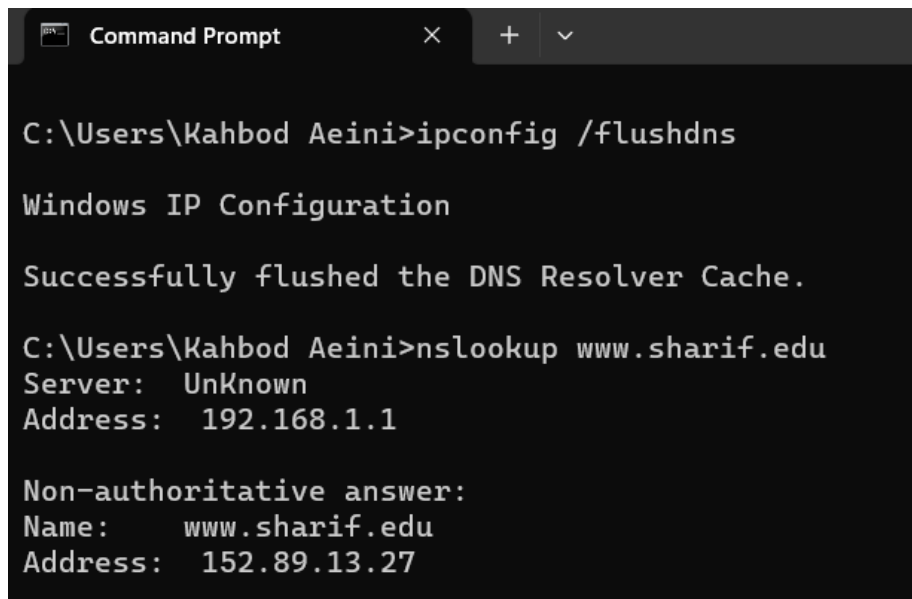


شکل ۱۴: کامند اجرا شده در Telnet

۳ بخش سوم (بررسی درخواست‌ها و پاسخ‌های DNS)

۱.۳

در اسکرین شات زیر، مراحل اولیه‌ی انجام آزمایش را می‌توانیم ببینیم.



```
Command Prompt

C:\Users\Kahbod Aeini>ipconfig /flushdns

Windows IP Configuration

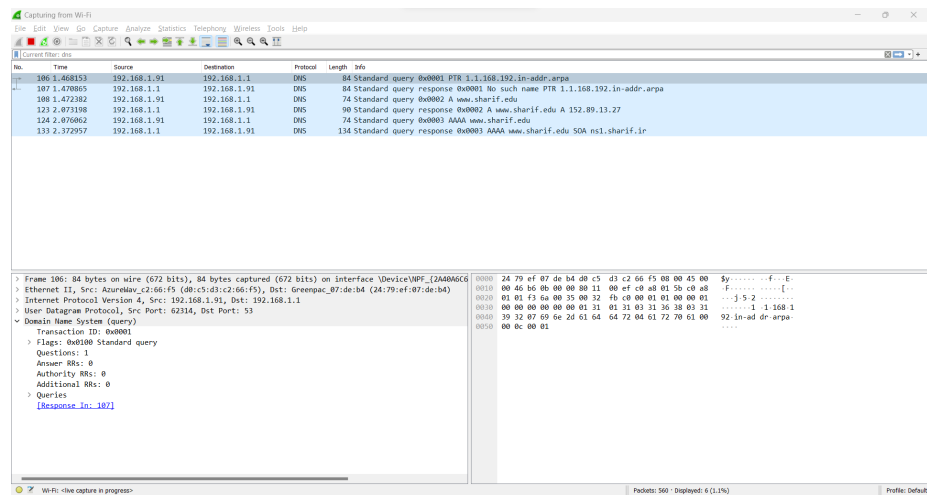
Successfully flushed the DNS Resolver Cache.

C:\Users\Kahbod Aeini>nslookup www.sharif.edu
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: www.sharif.edu
Address: 152.89.13.27
```

شکل ۱۵: پاک کردن cache در Host با استفاده از command prompt و انجام nslookup

حال به بررسی این درخواست در wireshark می‌پردازیم.

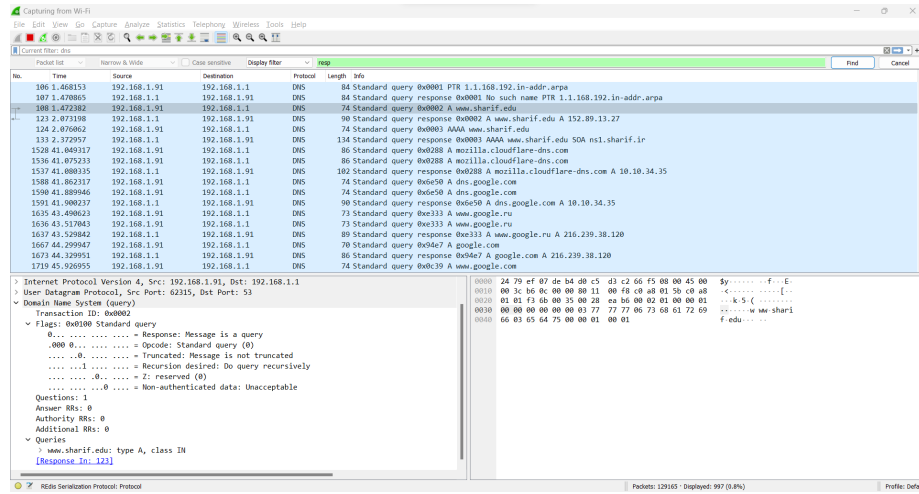


شکل ۱۶: بررسی درخواست DNS به سایت شریف در wireshark

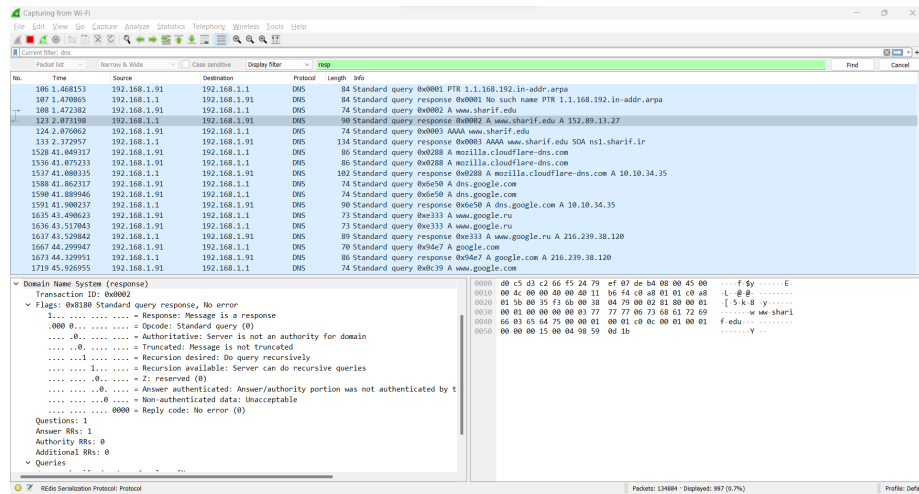
همان‌طور که در اسکرین‌شات دیدیم، درخواست‌ها به ip سرور مبدا یعنی ۹۱.۱.۱۶۸.۱۹۲ به آدرس ۱.۱.۱۶۸.۱۹۲ ارسال می‌شوند.

۲.۳

ابتدا در اسکرین‌شات‌های زیر پیام‌های query (request) و response (reply) را می‌بینیم و سپس به تحلیل هدرهای آن‌ها می‌پردازیم.



شکل ۱۷: request or query



شکل ۱۸: reply or response

هدرها شامل دو بخش اصلی ID Transaction و Flags می‌شوند که در ادامه به توصیف هر کدام می‌پردازیم.

ID Transaction

شناسه ۱۶ بیتی اختصاص داده شده توسط برنامه‌های که هر نوع درخواستی را ایجاد می‌کند. این شناسه از پاسخ مربوطه کپی می‌شود و می‌تواند توسط متقاضی برای مطابقت دادن پاسخ‌ها با درخواست‌ها استفاده شود.

Flags

این قسمت شامل چند بخش دیگر است که با نام‌ها و کاربرد‌های زیر در تصویر دیده می‌شوند:

۱. Response

یک مقدار تک بیتی است که مشخص می‌کند که پیام از نوع درخواست (۰) و یا پاسخ (۱) است.

۲. Opcode

بخش ۴ بیتی است که مشخص می‌کند چه نوع درخواستی در پیام وجود دارد و اگر درخواست باشد برابر صفر خواهد بود. query standard مانند تصویر

۳. Truncated

تک بیتی که نشان می‌دهد پیام کوتاه شده است یا خیر.

۴. Desired Recursion

این بیت نام سرور را برای پیگیری جستجو به صورت بازگشتی هدایت می‌کند. که برای استفاده در آینده رزرو می‌شود. Z و بیت

این بخش‌ها در هر دو نوع هدر مشترک هستند، هدر پاسخ اطلاعات زیر را نیز دارد:

۱. Authoritative

این بیت فقط در پاسخ‌ها معنی‌دار است و مشخص می‌کند که سرور پاسخ‌دهنده یک مرجع برای نام دامنه در بخش سوال باشد.

۲. Available Recursion

این بیت در یک پاسخ تنظیم شده یا پاک می‌شود و نشانگر این است که آیا پشتیبانی درخواست بازگشتی در سرور در دسترس است یا خیر. پشتیبانی درخواست بازگشتی اختیاری است.

۳. code Response

این قسمت ۴ بیتی می‌تواند مقادیر زیر را بگیرد:

صفر - خطایی وجود ندارد.

یک - خطای فرمت: سرور قادر به تفسیر درخواست نبود.

دو - خرابی سرور: server Name به دلیل مشکلی نتوانست درخواست را پردازش کند.

سه - خطای نام: نام دامنه‌ی ارجاع شده در درخواست وجود ندارد.

چهار - اجرا نشده: server Name این نوع درخواست را پردازش نمی‌کند.

پنج - رد شده: نام سرور از انجام عملیات به دلایل policy خودداری می‌کند.