



آزمایشگاه شبکه‌های کامپیوتری

آزمایش دوم

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

نیم سال دوم ۱۴۰۰-۱۴۰۱

استاد:

جناب آقای دکتر صفایی

اعضای گروه:

محمد سپهر 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، مثلاً 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 پرکاربردترین پروتکل لایه کاربرد **HTTP** بوده است. همچنین شاهد این هستیم که در زیر شاخه پروتکل‌های لایه کاربرد وابسته به **UDP** پرکاربردترین (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	1,113k	37	1382703	1,113k
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.

No.	Time	Source	Destination	Protocol	Length	Info
16	0.000000000	10.0.2.15	10.0.2.15	HTTP	479	GET / HTTP/1.1
17	0.000000000	10.0.2.15	10.0.2.15	HTTP	2199	HTTP/1.1 200 OK (text/html)
18	0.000000000	10.0.2.15	10.0.2.15	HTTP	514	GET /html/portlet/ext/chat/css/jquery.gritter.css HTTP/1.1
19	0.000000000	10.0.2.15	10.0.2.15	HTTP	537	GET /portal/css/cachedThemeId=sharifcolorSchemeId=01&t=1628440472580 HTTP/1.1
20	0.000000000	10.0.2.15	10.0.2.15	HTTP	2088	HTTP/1.1 200 OK (text/css)
21	0.000000000	10.0.2.15	10.0.2.15	HTTP	589	GET /html/css/general_reportal2.css HTTP/1.1
22	0.000000000	10.0.2.15	10.0.2.15	HTTP	514	GET /html/css/bootstrap/css/bootstrap.rtl.min.css HTTP/1.1
23	0.000000000	10.0.2.15	10.0.2.15	HTTP	589	GET /html/css/bootstrap/css/font-awesome.css HTTP/1.1
24	0.000000000	10.0.2.15	10.0.2.15	HTTP	499	GET /html/css/general_reportal.css HTTP/1.1
25	0.000000000	10.0.2.15	10.0.2.15	HTTP	562	GET /html/portlet/ext/slide_content_image/css.jsp?themeId=sharifcolorSchemeId=01&t=1628440469954 HTTP/1.1
26	0.000000000	10.0.2.15	10.0.2.15	HTTP	2943	HTTP/1.1 200 OK (text/css)
27	0.000000000	10.0.2.15	10.0.2.15	HTTP	5857	HTTP/1.1 200 OK (text/css)
28	0.000000000	10.0.2.15	10.0.2.15	HTTP	8916	HTTP/1.1 200 OK (text/css)

شکل ۲: اولین درخواست **HTTP GET**



آزمایش دوم

No.	Time	Source	Destination	Protocol	Length	Info
48	2.359732768	10.0.2.15	81.31.186.20	HTTP	478	GET /home HTTP/1.1
49	3.360702350	10.0.2.15	81.31.186.20	HTTP	514	GET /html/portlet/mstr/chai/css/jquery.gritter.css HTTP/1.1
50	3.360905638	10.0.2.15	81.31.186.20	HTTP	537	GET /c/portal/css/cached?themeId=sharif&colorSchemeId=81at=1628448472589 HTTP/1.1
51	3.361115486	10.0.2.15	81.31.186.20	HTTP	2688	HTTP/1.1 200 OK (text/css)
52	3.36128454	10.0.2.15	81.31.186.20	HTTP	588	GET /html/css/general/ecomportal2.css HTTP/1.1
53	3.361399240	10.0.2.15	81.31.186.20	HTTP	514	GET /html/css/bootstrap/css/bootstrap-rtl.min.css HTTP/1.1
54	3.361533918	10.0.2.15	81.31.186.20	HTTP	588	GET /html/css/bootstrap/css/font-awesome.css HTTP/1.1
55	3.361734970	10.0.2.15	81.31.186.20	HTTP	499	GET /html/css/general/ecomportal.css HTTP/1.1
56	3.361115486	10.0.2.15	81.31.186.20	HTTP	582	GET /html/portlet/mstr/cslide_content_image/css.jsp?themeId=sharif&colorSchemeId=81at=1628448469954 HTTP/1.1
57	4.021681444	81.31.186.20	10.0.2.15	HTTP	2943	HTTP/1.1 200 OK (text/css)
58	4.031938093	81.31.186.20	10.0.2.15	HTTP	5857	HTTP/1.1 200 OK (text/css)
59	4.035284476	81.31.186.20	10.0.2.15	HTTP	3916	HTTP/1.1 200 OK (text/css)

Frame 36: 11950 bytes on wire (95000 bits), 11950 bytes captured (95000 bits) on interface eth0, id 0

Interface id 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 3, 2022 19:40:09.601833706 EST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 564348179.602941352 seconds

[Time delta from previous captured frame: 0.001049177 seconds]

[Time delta from previous displayed frame: 0.876629628 seconds]

[Time since reference or first frame: 3.359732768 seconds]

Frame Number: 36

Frame Length: 11950 bytes (95000 bits)

Capture Length: 11950 bytes (95000 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data:text-lines]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || top.port == 80 || http2]

Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_43:73:bc (08:00:27:43:73:bc)

Internet Protocol Version 4, Src: 81.31.186.20, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 80, Dst Port: 39564, Seq: 39567939, Ack: 2296291943, Len: 11896

[9 Reassembled TCP Segments (7233 bytes): #28(17), #22(4388), #24(5648), #26(7380), #28(6789), #30(18228), #32(11689), #34(13148), #36(11896)]

Hypertext Transfer Protocol

شکل ۳: پاسخ OK HTTP نظیر درخواست قبلی

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

No.	Time	Source	Destination	Protocol	Length	Info
15	2.359732768	10.0.2.15	81.31.186.20	TCP	60	80 --> 39564 [SYN, ACK] Seq=395536801 Ack=2296291943 Win=65535 Len=0
16	2.360702350	10.0.2.15	81.31.186.20	TCP	54	39564 --> 80 [ACK] Seq=2296291943 Ack=395536802 Win=64248 Len=0
17	2.360905638	10.0.2.15	81.31.186.20	HTTP	478	GET /home HTTP/1.1
18	2.361115486	10.0.2.15	81.31.186.20	TCP	60	80 --> 39564 [ACK] Seq=395536802 Ack=2296292368 Win=65535 Len=0
19	2.36128454	10.0.2.15	81.31.186.20	TCP	71	80 --> 39564 [ACK] Seq=395536802 Ack=2296292368 Win=65535 Len=17 [TCP segment of a reassembled PDU]
20	2.361399240	10.0.2.15	81.31.186.20	TCP	54	39564 --> 80 [ACK] Seq=2296292368 Ack=395536819 Win=64223 Len=0
21	2.361533918	10.0.2.15	81.31.186.20	TCP	4334	80 --> 39564 [ACK] Seq=395536819 Ack=2296292368 Win=65535 Len=4300 [TCP segment of a reassembled PDU]
22	2.361734970	10.0.2.15	81.31.186.20	TCP	54	39564 --> 80 [ACK] Seq=2296292368 Ack=395540399 Win=61328 Len=0
23	2.361899240	10.0.2.15	81.31.186.20	TCP	5884	80 --> 39564 [ACK] Seq=395540399 Ack=2296292368 Win=65535 Len=5840 [TCP segment of a reassembled PDU]
24	2.362053918	10.0.2.15	81.31.186.20	TCP	54	39564 --> 80 [ACK] Seq=2296292368 Ack=395540429 Win=58400 Len=0
25	2.362218192	10.0.2.15	81.31.186.20	TCP	7354	80 --> 39564 [ACK] Seq=395540429 Ack=2296292368 Win=65535 Len=7300 [TCP segment of a reassembled PDU]
26	2.362382466	10.0.2.15	81.31.186.20	TCP	54	39564 --> 80 [ACK] Seq=2296292368 Ack=395553539 Win=52568 Len=0

Arrival Time: Mar 3, 2022 19:47:59.682941582 EST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 564348179.682941352 seconds

[Time delta from previous captured frame: 0.000718937 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 2.937878182 seconds]

Frame Number: 15

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || top.port == 80 || http2]

Ethernet II, Src: PcsCompu_43:73:bc (08:00:27:43:73:bc), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 81.31.186.20

Transmission Control Protocol, Src Port: 39564, Dst Port: 80, Seq: 2296291942, Len: 0

Source Port: 39564

Destination Port: 80

[Stream index: 6]

[TCP Segment Len: 0]

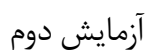
Sequence Number: 2296291942

(Next Sequence Number: 2296291943)

Acknowledgment Number: 0

شکل ۴: اولین بسته SYN TCP نظیر درخواست قبلی

۳. مطابق شکل های ۵ و ۶ 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 آی پی 81.31.186.20 دریافت شده است.



شکل ۵: کوئری DNS

شکل ۶: 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 انتخاب Export Packet Bytes عکس‌ها را ذخیره می‌کنیم.

شکل ۷: مشاهده شکل‌های دانلود شده از سرور



آزمایش دوم

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



شکل ۸: عکس‌های دانلود شده از سرور



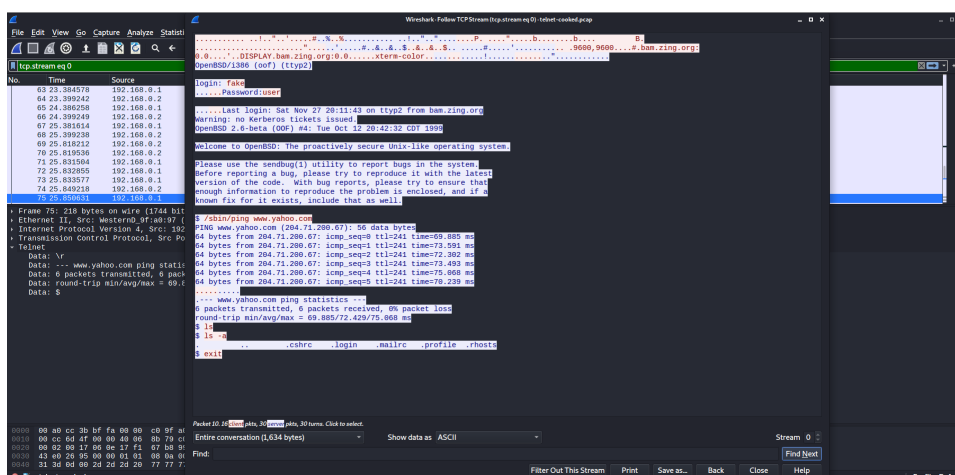
۲ سوالات بخش دوم

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	60	1550 → 23 [ACK] Seq=2579865836 Win=32128 Len=0 MSS=1460 Sack_Flags=1 TSval=18233651 TSecr=18233651
2	0.000225	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [FIN, ACK] Seq=481695548 Ack=2579865837 Wlen=37376 Len=0 MSS=1440 WS=1 TSval=2467372 TSecr=18233651
3	0.000272	192.168.0.2	192.168.0.1	TCP	60	1550 → 23 [ACK] Seq=2579865837 Ack=481695558 Wlen=32128 Len=0 TSval=18233651 TSecr=2467372
4	0.004169	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150320	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150462	192.168.0.2	192.168.0.1	TCP	60	1550 → 23 [ACK] Seq=2579865864 Ack=481695553 Wlen=32128 Len=0 TSval=18233651 TSecr=2467372
7	0.150974	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
8	0.151346	192.168.0.1	192.168.0.2	TCP	60	23 → 1550 [ACK] Seq=481695553 Ack=2579865867 Wlen=17376 Len=0 TSval=2467372 TSecr=18233651
9	0.151857	192.168.0.1	192.168.0.2	TELNET	91	Telnet Data ...
10	0.151865	192.168.0.2	192.168.0.1	TELNET	138	Telnet Data ...
11	0.154984	192.168.0.1	192.168.0.2	TCP	60	23 → 1550 [ACK] Seq=481695578 Ack=2579865931 Wlen=17312 Len=0 TSval=2467372 TSecr=18233651
12	0.155577	192.168.0.1	192.168.0.2	TELNET	64	Telnet Data ...
13	0.155656	192.168.0.2	192.168.0.1	TELNET	75	Telnet Data ...

شکل ۹: وضعیت کلی پکت‌های ارسالی Telnet

برای دو قسمت بعدی، پکت‌های نوع **TELNET** را فیلتر کرده، روی اولین مورد کلیک راست کرده و برای TCP Stream و Follow 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:



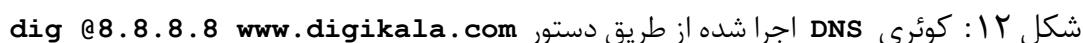
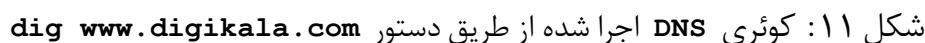
آزمایش دوم

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

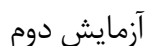


۱. مطابق شکل ۱۱ دستور را در یک سیستم عامل لینوکسی و برای سایت www.digikala.com انجام داده‌ایم. از آن جایی که فایل `/etc/resolv.conf` سیستم ما به صورت

تنظیم شده بود، این کوثری 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 می شود که این موضوع را در شکل ۱۲ مشاهده می کنید.



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.



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 کوثری 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 اوری، برخورد نکرده است.

```

#ids
No.    Time      Source          Destination      Protocol Length Info
--
123.58.423591526 18.0.2.15      192.168.1.1     DNS             89 Standard query 0x4008 A www.digipala.com GP
124.58.455424688 192.168.1.1     18.0.2.15      DNS             458 Standard query response 0x4008 A www.digipala.com CHWOW points.digitalcloud.com A 91.99.72.75 A 94.182.187.148 A 5.166.243.80 A 17
...
+ User Datagram Protocol, Src Port: 53, Dst Port: 38286
+ Domain Name System (response)
+ Transaction ID: 0x4008
+ Flags: 0x10 Standard query response, No error
1... .. Response: Message is a response
... .. 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
... ..0... .. Opcode: Reply code: No error (0)

Questions: 1
Answer RRs: 22
Authority RRs: 0
Additional RRs: 1
+ Queries
+ www.digipala.com: type CHWOW, class IN, owner points.digitalcloud.com
+ points.digitalcloud.com: type A, class IN, addr 91.99.72.75
+ points.digitalcloud.com: type A, class IN, addr 94.182.187.148
+ points.digitalcloud.com: type A, class IN, addr 5.166.243.80
+ points.digitalcloud.com: type A, class IN, addr 174.216.248.251
+ points.digitalcloud.com: type A, class IN, addr 92.114.19.28
+ points.digitalcloud.com: type A, class IN, addr 24.218.255.8
0840 61 6c 61 83 0f 6d 08 08 01 08 01 60 6c 80 05 ala com ...

```

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