

دستور کار شماره ۴ آزمایشگاه شبکه‌های کامپیوتری

نگار موقتیان – ۹۸۳۱۰۶۲

تینا توحیدخواه – ۹۸۳۱۱۳۴

گروه ۶ – چهارشنبه ۱۶:۳۰

۱: داده‌های مشاهده شده را می‌توان به چند بخش تقسیم کرد:

ابتدا لیستی از Host های درخواست داده شده و IP آن‌ها

```
# Hosts
#
# 170 entries.

0.0.0.0 c142a355-11d8-471c-91b9-f9994596b2ef.local
151.101.242.167 twitch.map.fastly.net
172.217.19.5 googlemail.l.google.com
78.157.43.149 logo.samandehi.ir
52.25.210.71 edger-edger-ra7qmuyuwxs-482101627.us-west-2.elb.amazonaws.com
52.39.100.161 pubsub-edge.twitch.tv
50.112.164.229 science-edge-external-prod-73889260.us-west-2.elb.amazonaws.com
87.250.250.119 mc.yandex.ru
52.88.209.254 irc-ws.chat.twitch.tv
13.32.121.25 d36mepituis1gg.cloudfront.net
13.32.99.90 sb.scorecardresearch.com
173.194.188.102 r1.sn-4g5ednss.gvt1.com
18.66.242.68 d2v02itv0y9u9t.cloudfront.net
142.250.186.173 accounts.google.com
52.10.214.44 edger-edger-ra7qmuyuwxs-482101627.us-west-2.elb.amazonaws.com
77.88.21.119 mc.yandex.ru
23.160.0.0 global.poe.live-video.net
18.66.248.34 certify-js.alexametrics.com
3.0.161.212 census.ap-southeast-1.nielsencollections.com
35.160.44.237 pubsub-edge.twitch.tv
34.211.213.19 passport.twitch.tv
34.215.74.40 pubsub-edge.twitch.tv
172.23.141.69 446721c4-9368-45b0-b5e8-ad380803ddea.local
18.66.139.97 dxtkri2c61io4.cloudfront.net
185.147.179.174 hajifirouz12.cdn.asset.aparat.com
52.24.75.179 edger-edger-ra7qmuyuwxs-482101627.us-west-2.elb.amazonaws.com
52.222.247.124 d186rixkn5ruba.cloudfront.net
44.225.18.119 science-edge-external-prod-73889260.us-west-2.elb.amazonaws.com
142.250.181.142 redirector.gvt1.com
18.66.139.122 dxtkri2c61io4.cloudfront.net
99.181.64.219 video-edge-1ff2fc.fra05.abs.hls.ttvnw.net
172.23.142.186 15b7f54b-e18d-4849-8766-2d73a2dd716d.local
192.108.239.254 usher.ttvnw.net
185.147.178.34 live.cdn.asset.aparat.com
13.32.99.104 certify.alexametrics.com
52.33.249.131 irc-ws.chat.twitch.tv
37.128.150.243 twitchinstagram.polymedia.nl
35.160.253.116 irc-ws.chat.twitch.tv
216.58.212.162 adservice.google.com
52.10.121.29 passport.twitch.tv
108.157.4.78 d2926jmsihu4k.cloudfront.net
185.147.179.236 ads.cdn.asset.aparat.com
18.66.248.48 d18748y6j3mqpw.cloudfront.net
104.18.16.52 cdn.streamelements.com
54.69.142.143 edger-edger-ra7qmuyuwxs-482101627.us-west-2.elb.amazonaws.com
185.147.178.35 live.cdn.asset.aparat.com
13.32.99.105 sb.scorecardresearch.com
```

سپس لیستی از سرویس ها که در جلوی هر کدام شماره بسته و نوع پروتکل استفاده شده

```
# Services
#
# 6073 entries.

entomb 775/tcp
acmaint-transd 775/udp
3m-image-lm 1550/tcp
3m-image-lm 1550/udp
ansysli 2325/tcp
ansysli 2325/udp
pnbscada 3875/tcp
pnbscada 3875/udp
opcon-xps 3100/tcp
opcon-xps 3100/udp
br-channel 5425/tcp
br-channel 5425/udp
lm-x 6200/tcp
lm-x 6200/udp
vrace 9300/tcp
vrace 9300/udp
is99c 379/tcp
is99c 379/udp
resacommunity 1154/tcp
resacommunity 1154/udp
bandwiz-system 1929/tcp
bandwiz-system 1929/udp
sms-remctrl 2704/tcp
sms-remctrl 2704/udp
twrpc 3479/tcp
twrpc 3479/udp
infobright 5029/tcp
infobright 5029/udp
affiliate 6579/tcp
affiliate 6579/udp
paycash-wbp 8129/tcp
paycash-wbp 8129/udp
entextlow 12004/tcp
entextlow 12004/udp
nlogin 758/tcp
nlogin 758/udp
virtual-places 1533/tcp
virtual-places 1533/udp
sdhelp 2308/tcp
sdhelp 2308/udp
trap-port-mom 3858/tcp
trap-port-mom 3858/udp
tll-telnet 3083/tcp
tll-telnet 3083/udp
foresyte-sec 5408/tcp
foresyte-sec 5408/udp
callwaveiam 9283/tcp
callwaveiam 9283/udp
bf-game 25954/udp
kopek-httphead 27504/tcp
kopek-httphead 27504/udp
srssend 362/tcp
srssend 362/udp
trim 1137/tcp
trim 1137/udp
```

آدرس های فیزیکی Ethernet های درخواست شده و به دنبال آن سازنده ها

```
# Ethernet addresses
#
# 182 entries.

33:33:ff:53:c7:da IPv6mcast_ff:53:c7:da
01:00:1d:42:00:00 Cabletron-PC-OV-Bridge-discover-(on-demand)
01:80:c2:00:00:46 All-Edge-RBridges
09:00:09:00:00:01 HP-Probe
01:80:c2:00:00:1d ESIS-all-multicast-capable-IS's
01:80:c2:00:00:1e Token-Ring-all-DTR-Concentrators
09:00:87:80:ff:ff Xyplex-Terminal-Servers
01:10:18:01:00:02 All-FCF-MACs
09:00:2b:00:00:04 DEC-MAP-(or-OSI?)-End-System-Hello?
03:00:00:00:40:00 IMPL-Server
09:00:7c:01:00:01 Vitalink-DLS-Multicast
09:00:4c:00:00:06 BICC-Local-bridge-STA-802.1(D)-Rev6
01:00:81:00:00:00 Nortel-Network-Management
09:00:2b:00:00:02 DEC-VAXELN?
09:00:07:ff:ff:ff AppleTalk-broadcast-address
01:80:c2:00:00:02 Slow-Protocols
09:00:0d:02:ff:ff ICL-Oslan-Service-discover-only-on-boot
00:e0:2b:00:00:00 Extreme-EDP
48:2a:e3:56:ca:71 WistronI_56:ca:71
03:00:00:00:01:00 OSI-All-IS-Token-Ring-Multicast
00:e0:2b:00:00:06 Extreme-EAPS-SL
01:0f:ff:c1:02:c0 FP-Flood-to-all-Fabrics
01:80:c2:00:00:03 Nearest
cf:00:00:00:00:00 Ethernet-Configuration-Test-protocol-(Loopback)
09:00:2b:00:00:06 DEC-CSMA/CD-Encryption?
01:00:81:00:01:01 Nortel-autodiscovery
00:e0:2b:00:00:02 Extreme-ESRP-Client
33:33:ff:6d:c5:28 IPv6mcast_ff:6d:c5:28
09:00:0d:02:0a:38 ICL-Oslan-Service-discover-only-on-boot
09:00:0d:02:0a:3c ICL-Oslan-Service-discover-only-on-boot
01:80:c2:00:00:42 All-Egress-RBridges
01:00:1d:52:00:00 Cabletron-PC-OV-MMAC-discover-(on-demand)
00:e0:2b:00:00:01 Extreme-EEP
28:c7:ce:0d:f6:81 Cisco_0d:f6:81
3c:7c:3f:ea:5f:a2 3c:7c:3f:ea:5f:a2
18:8b:45:5a:72:41 Cisco_5a:72:41
ab:00:00:02:00:00 DEC-MOP-Remote-Console
09:00:7c:05:00:02 Vitalink-Network-Validation-Message
01:00:5e:40:98:8f IPv4mcast_40:98:8f
01:10:18:01:00:00 All-FCoE-MACs
01:dd:00:ff:ff:ff Ungermann-Bass-boot-me-requests
03:00:00:00:00:02 Locate-Directory-Server
01:e0:2f:00:00:02 DOCSIS-CMTS
33:33:00:00:00:fb IPv6mcast_fb
78:24:af:bd:0b:a4 AsustekC_bd:0b:a4
00:e0:4c:68:1c:5f RealtekS_68:1c:5f
01:80:c2:00:00:15 ISIS-all-level-2-IS's
09:00:4c:00:00:0f BICC-Remote-bridge-ADAPTIVE-ROUTING
09:00:2b:04:00:00 DEC-Local-Area-System-Transport-(LAST)?
03:00:00:00:00:80 Active-Monitor
88:d7:f6:da:02:dc AsustekC_da:02:dc
09:00:1e:00:00:00 Apollo-DOMAIN
01:00:0c:cc:cc:cc CDP/VTP/DTP/PAAP/INDI D
```

۲: در ادامه ۴ آدرس به عنوان نمونه آمده است :

00:08:e2 Cisco Systems, Inc

70:35:09 Cisco Systems, Inc

00:0f:23 Cisco Systems, Inc

00:be:75 Cisco Systems, Inc

۳: ابتدا سلسله ی پروتکل ها به تفکیک لایه ها نمایش داده شده است و سپس در هر ستون اطلاعاتی درباره ی هر پروتکل برای مثال در ستون دوم از چپ نشان داده شده است که چند درصد از بسته ها از پروتکل مشخص شده استفاده میکنند و اطلاعاتی از این دست.

Wireshark - Protocol Hierarchy Statistics - Local Area Connection								
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	205474	100.0	174065118	3558 k	0	0	0
Ethernet	100.0	205474	1.7	2876636	58 k	0	0	0
Logical-Link Control	0.1	228	0.0	11558	236	0	0	0
Spanning Tree Protocol	0.1	195	0.0	6825	139	195	6825	139
Dynamic Trunk Protocol	0.0	26	0.0	832	17	13	416	8
VSS-Monitoring ethernet trailer	0.0	13	0.0	26	0	13	26	0
Cisco Discovery Protocol	0.0	7	0.0	3052	62	7	3052	62
Internet Protocol Version 6	0.1	166	0.0	6640	135	0	0	0
User Datagram Protocol	0.1	153	0.0	1224	25	0	0	0
Simple Service Discovery Protocol	0.0	12	0.0	1416	28	12	1416	28
Multicast Domain Name System	0.0	83	0.0	7210	147	83	7210	147
Link-local Multicast Name Resolution	0.0	7	0.0	222	4	7	222	4
DHCPv6	0.0	51	0.0	4575	93	51	4575	93
Internet Control Message Protocol v6	0.0	13	0.0	256	5	13	256	5
Internet Protocol Version 4	82.9	170397	2.0	3408172	69 k	0	0	0
User Datagram Protocol	1.1	2231	0.0	17848	364	1	8	0
Simple Service Discovery Protocol	0.5	1101	0.1	151457	3096	1101	151457	3096
NetBIOS Name Service	0.0	64	0.0	4314	88	64	4314	88
NetBIOS Datagram Service	0.0	6	0.0	1214	24	0	0	0
SMB (Server Message Block Protocol)	0.0	6	0.0	722	14	0	0	0
SMB MailSlot Protocol	0.0	6	0.0	150	3	0	0	0
Microsoft Windows Browser Protocol	0.0	6	0.0	206	4	6	206	4
Multicast Domain Name System	0.3	585	0.0	38178	780	585	38178	780
Local Service Discovery	0.0	8	0.0	952	19	8	952	19
Link-local Multicast Name Resolution	0.0	71	0.0	2410	49	71	2410	49
Dynamic Host Configuration Protocol	0.0	26	0.0	7838	160	26	7838	160
Domain Name System	0.1	187	0.0	13005	265	187	13005	265
Data	0.1	182	0.1	191580	3916	182	191580	3916
Transmission Control Protocol	81.8	168087	95.2	165707347	3387 k	127114	118141175	2415 k
Transport Layer Security	21.4	43911	79.1	137680211	2814 k	40146	88707874	1813 k
Malformed Packet	0.0	2	0.0	0	0	2	0	0
Hypertext Transfer Protocol	0.1	239	8.2	14251149	291 k	147	62074	1269
Portable Network Graphics	0.0	2	0.0	6908	141	2	7464	152
Media Type	0.0	41	0.5	880035	17 k	41	446209	9122
Line-based text data	0.0	9	0.0	81314	1662	9	26679	545
JPEG File Interchange Format	0.0	2	0.0	10324	211	2	10884	222
JavaScript Object Notation	0.0	1	0.0	2849	58	1	2849	58
ISO/IEC 13818-1	33.8	69525	7.5	13070700	267 k	33	13081953	267 k
Packetized Elementary Stream	1.8	3701	0.0	0	0	0	0	0
Moving Picture Experts Group Audio	0.3	534	0.0	0	0	0	0	0

No display filter.

Close

Copy

Help

۴: ۸۲,۹ درصد. ممکن است این سوال مطرح شود که چرا با وجود IPv6 درصد بالایی از بسته ها تحت پروتکل IPv4 است. دلیل آن را میتوان هزینه بر بودن انتقال شرکت ها از IPv4 به IPv6 دانست. بنابراین بسیاری از شرکت ها ترجیح می دهند بر بستر IPv4 بمانند.

۵:

در بالای صفحه سربرگ هایی مشاهده میشود که با استفاده از آن ها میتوان اطلاعاتی را که در ادامه به آن ها اشاره می شود به تفکیک پروتکل های مختلف بررسی و مشاهده کرد. اطلاعاتی که در هر سربرگ قابل دسترسی است شامل آدرس فیزیکی گره A و B تعداد بسته منتقل شده ، اندازه داده منتقل شده زمان شروع و مدت زمان انتقال و جهت انتقال داده و سرعت آن می شود .

Ethernet · 84 IPv4 · 157 IPv6 · 26 TCP · 231 UDP · 285													
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.23.141.69	8817	142.250.74.206	80	۲۰	7159	۱۰	1652	۱۰	5507	0.005478	178.7882	73	244
172.23.141.69	8829	74.125.98.40	80	۱۰	1831	۵	779	۵	1052	0.008809	0.2262	27 k	371
172.23.141.69	8828	74.125.98.38	80	۱۶۹	166 k	۵۵	3568	۱۱۴	163 k	0.192916	120.4581	236	101
172.23.141.69	8830	52.109.12.22	443	۵	433	۲	307	۲	126	1.686842	0.6413	3829	157
172.23.141.69	8831	52.109.12.22	443	۵	358	۲	232	۲	126	2.328738	0.3114	5960	323
172.23.141.69	8792	216.58.212.131	443	۹۰	18 k	۴۱	11 k	۴۹	6902	3.604782	374.6435	248	14
172.23.141.69	8826	142.250.181.132	443	۷	378	۷	378	۰	0	4.317356	18.9022	159	(

۴. در تصویر بالا یک نشست TCP مشخص شده است. این نشست دوطرفه بوده و در آن هر دو گره بسته هایی را ارسال و دریافت کرده اند.

۶: مانند بخش های بالا سربرگ هایی برای به تفکیک مشاهده کردن اطلاعاتی که در ادامه ذکر میشود برای هر پروتکل وجود دارد. اطلاعاتی که نشان میدهد از کدام پورت و آدرس چند بسته وبه چه اندازه ای دریافت و یا ارسال شده اند.

Ethernet · 39		IPv4 · 130		IPv6 · 19		TCP · 330		UDP · 306	
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes		
10.10.34.35	443	2328	-	0	2328				2328
13.32.99.23	443	44 k	92	21 k	172				22 k
13.32.99.104	443	18 k	22	10 k	24				8052
13.32.121.42	443	44 k	41	41 k	25				2960
13.49.134.162	443	360	360	-	0				0
13.107.42.16	443	60	60	-	0				0
18.66.112.113	443	18 k	22	14 k	28				4034
18.66.139.128	443	246 k	177	238 k	96				7808
18.66.242.48	443	119 k	115	115 k	49				4261
18.66.242.176	443	11 k	16	9758	12				1810
18.66.248.38	443	11 k	19	9370	18				2142
18.66.248.102	443	287 k	215	265 k	220				21 k
20.185.212.106	443	2965	2965	-	0				0
23.160.0.0	443	12 k	20	9714	22				3285
23.160.0.254	443	37 k	22	29 k	25				7957
23.205.249.88	443	6668	12	5495	10				1173
34.104.35.123	443	4117	12	1773	17				2344
37.128.150.243	443	7645	11	5964	18				1681
40.127.110.237	443	60	60	-	0				0
51.144.253.41	443	60	60	-	0				0
52.10.214.44	443	26 k	62	16 k	61				9079
52.39.100.161	443	62 k	145	28 k	201				34 k
52.109.12.22	443	4142	20	1260	21				2882
52.163.231.110	443	756	9	756	-				0
52.168.112.66	443	60	60	-	0				0
52.222.247.124	443	984 k	697	935 k	622				49 k
54.188.146.194	443	14 k	25	11 k	21				3652
54.200.107.114	443	439 k	219	30 k	162				409 k
54.251.90.32	443	8937	17	6355	16				2582
68.232.34.200	443	360	360	-	0				0
74.125.98.9	443	3173	1804	10	1369				1369
74.125.98.10	443	228	2	120	2				108
74.125.98.38	443	166 k	114	163 k	55				3568
74.125.98.40	443	1831	5	1052	5				779
74.125.98.47	443	3515	9	1962	10				1553

۷: با توجه به شکل بالا، در ادامه چهار نمونه از مقصد ها آمده است:

10.10.34.35:443

172.23.141.169:6573

172.23.141.169:9084

172.23.141.169:1333

۸: با توجه به شکل زیر دو گره آخر بیش ترین تبادل بسته ها را داشته اند بنابراین می توان نتیجه گرفت default gateway های شبکه هستند. چرا که بسته ها برای خروج از محیط private، غالباً به default gateway ها مراجعه میکنند (در این شبکه با توجه به بزرگ بودن شبکه دو default gateway داریم).

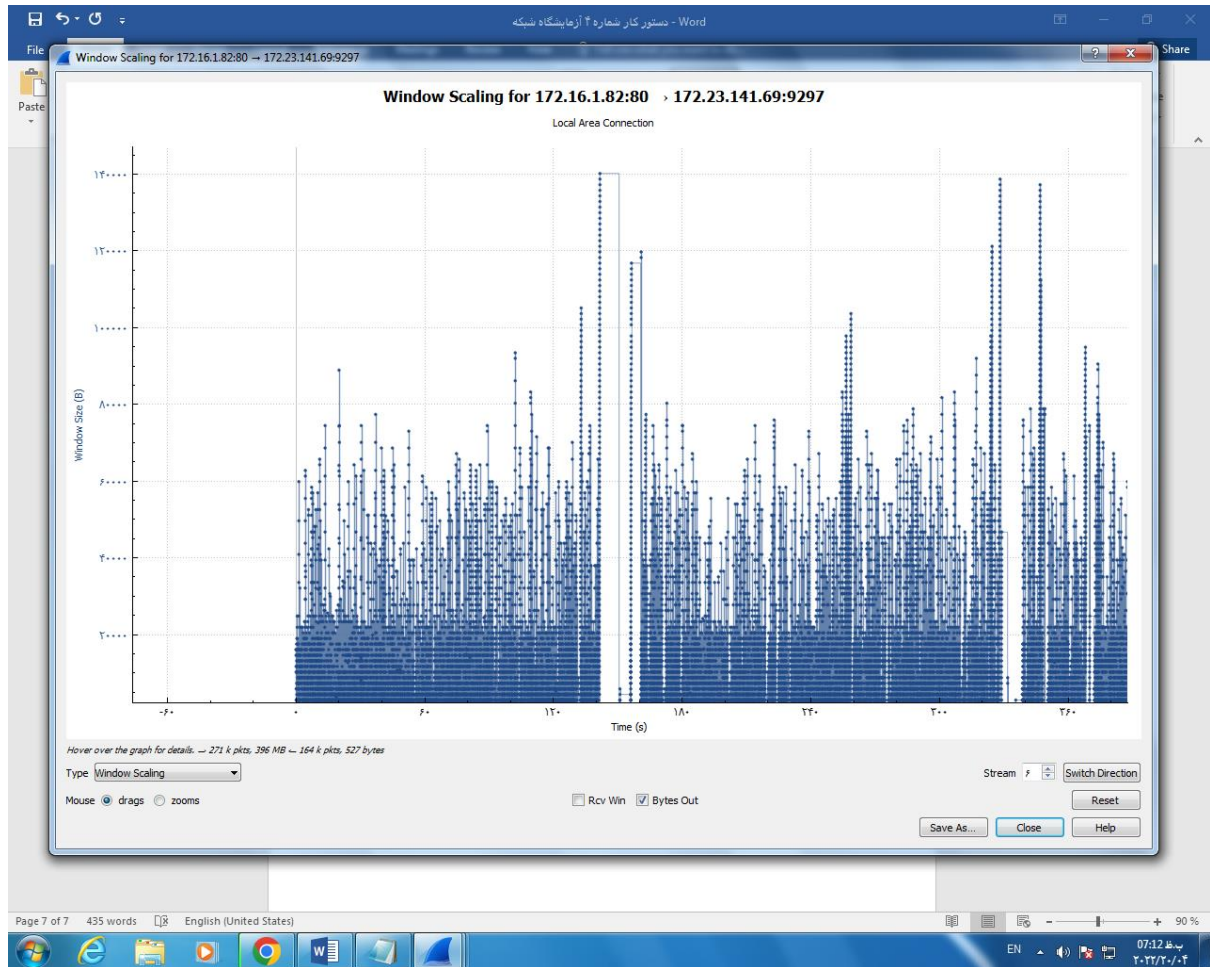
20:1a:00:93:c9:c8	1111+	307 k	1111+	307 k	*
98:29:a6:4a:0d:04	24,739	2108 k	24,720	2105 k	19
ff:ff:ff:ff:ff:ff	24,768	2096 k	*	0	24,768
78:24:af:bd:01:89	168,439	171 M	52,586	4877 k	115,853
04:6c:9d:27:9e:c2	168,522	171 M	116,052	166 M	52,470

۹: با توجه به اطلاعات قسمت Conversation، IP وبسایت دانشکده به صورت زیر می باشد:

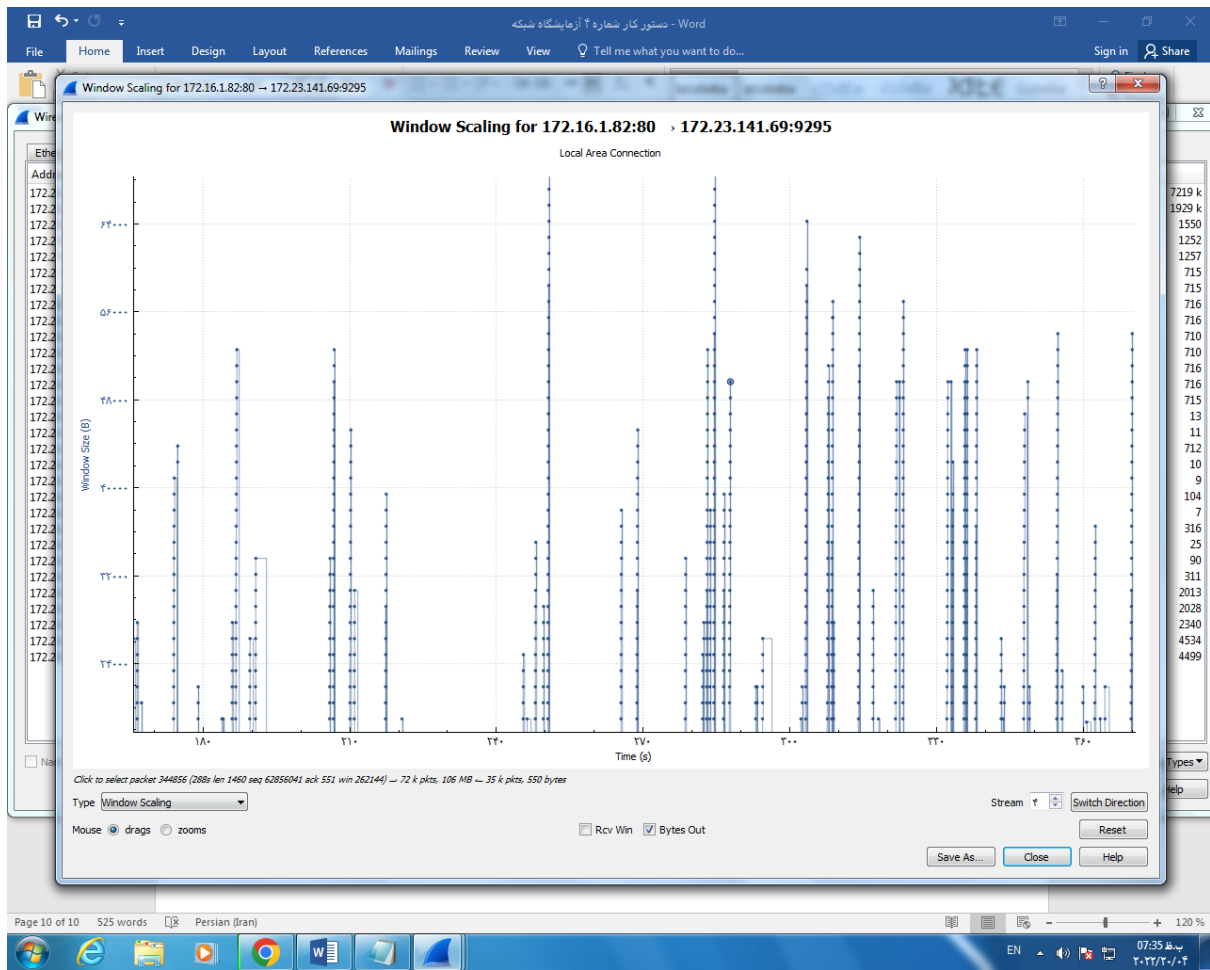
172.16.1.82

172.23.141.69	9311	172.16.1.194	443	QT	2/ k	20	5/11	TV	21 k	291.066056	60.6028	/53
172.23.141.69	9295	172.16.1.82	80	۱۳۴.۶۱۶	138 M	۴۴.۷۶۶	2696 k	۸۹.۸۵۰	135 M	9.766109	455.8450	47 k
172.23.141.69	9297	172.16.1.82	80	۵۲۶.۰۷۲	506 M	۱۹۹.۷۶۱	12 M	۳۲۶.۳۱۱	493 M	10.008118	455.5943	222 k

Window Scaling:

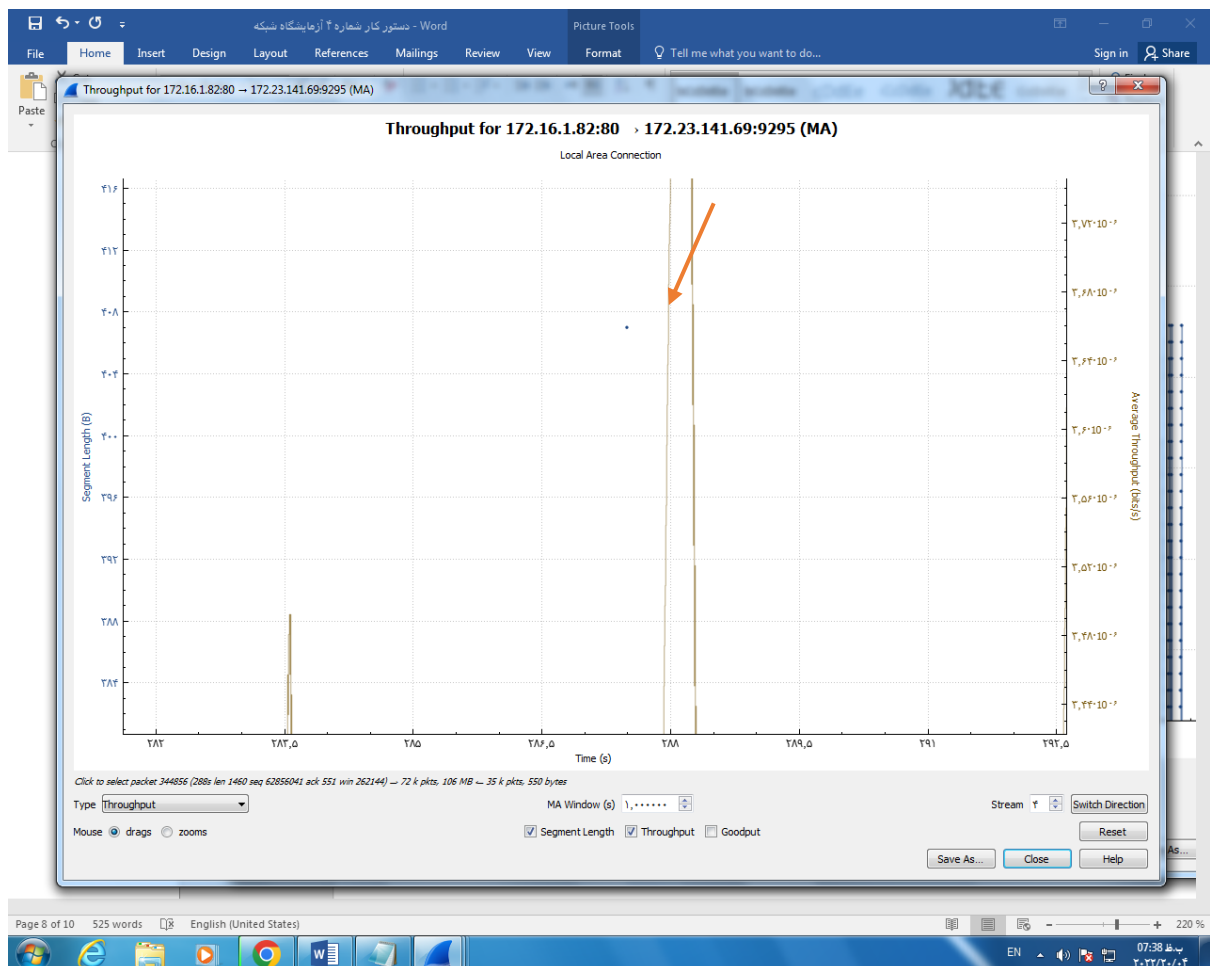


نقطه ای از نمودار Window Scaling:



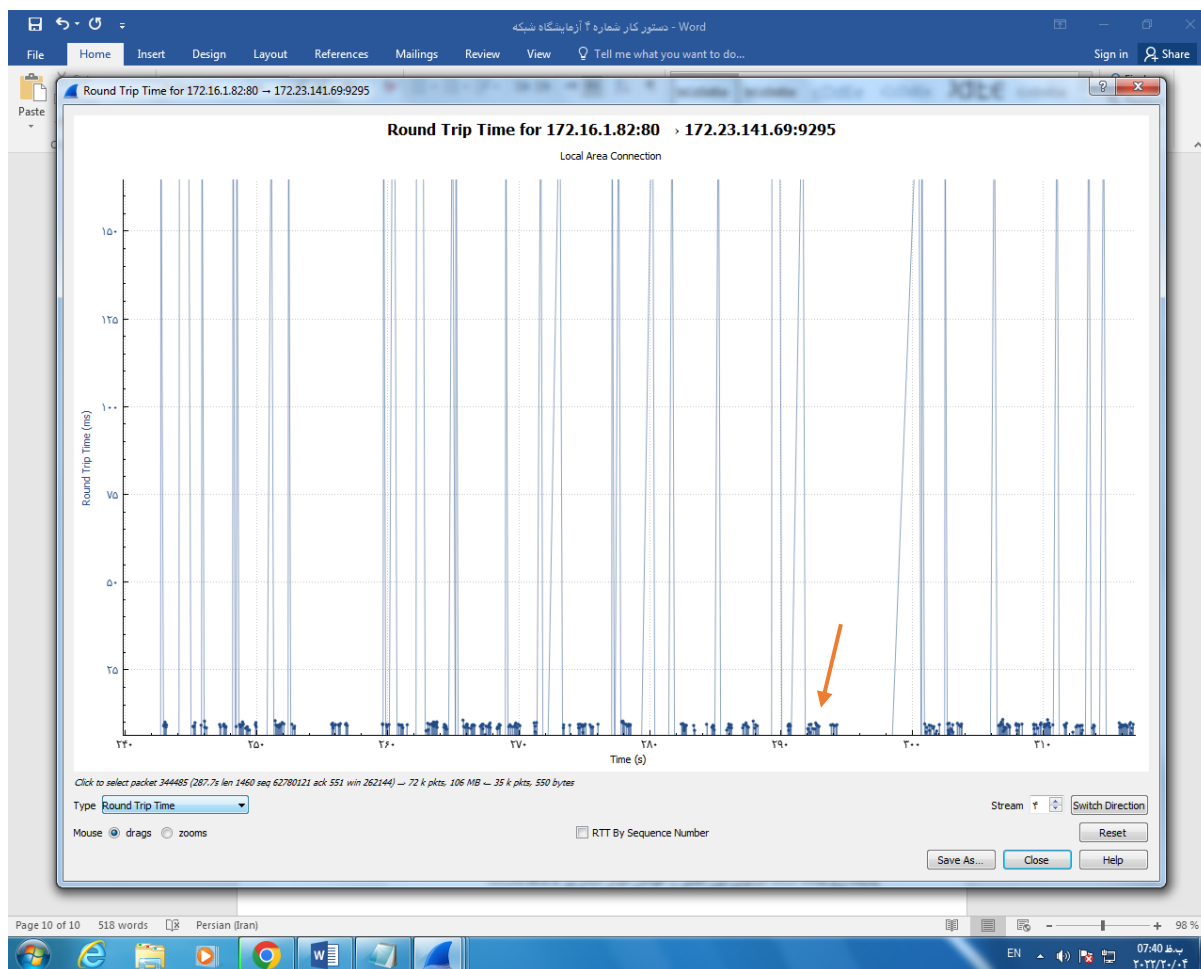
این نقطه ماکسیمم نمودار Window Scaling می باشد. در ادامه دیگر پارامترها برای این نقطه بررسی شده اند.

Through put:



در این نقطه با توجه به افزایش تعداد واحدهای ارسال شده همانطور که مشاهده می شود مقدار Throughput بالا است.

RTT:



همانطور که مشاهده می شود مقدار RTT در این نقطه بسیار کم است.