

## گزارش آزمایش تحلیل TCP با استفاده از Wireshark

مسیح دلفاردي ۹۸۳۱۰۷۹

امیر علی بلباسی ۹۸۳۱۱۰۹


### بخش ۱

#### سوال ۱ -

با باز کردن **resolve address** و پس از آن رفتن به :

- بخش **host** : مشاهده می شود که ادرس فیزیکی و نام شرکتی که ادرس فیزیکی متعلق به آن است در این بخش وجود

دارد

 Wireshark · Resolved Addresses

HostsPortsCapture File Comments

Search for entry (min 3 characters)All entries

Address	Name
c4:ff:bc:e0:00:00	viRaTec
70:b3:d5:4e:50:00	viZaarin
8c:1f:64:db:50:00	victtron
94.182.159.5	video-api.varzesh3.com
94.182.113.158	video-static.varzeshe3.com
94.182.113.155	video-static.varzeshe3.com
94.182.113.156	video-static.varzeshe3.com
94.182.113.147	video-static.varzeshe3.com
94.182.113.157	video-static.varzeshe3.com
94.182.113.154	video-static.varzeshe3.com
94.182.113.152	video.varzesh3.com
94.182.113.149	video.varzesh3.com
94.182.113.153	video.varzesh3.com

Close

- بخش **port** : اسامی که ان پورت را با انها می شناسند به همراه شماره پورت و نوع پورت نمایش می دهد

Hosts	Ports	Capture File Comments
Search for port or name		All entries ▾
Name	Port	Type
availant-mgr	1122	tcp
availant-mgr	1122	udp
murray	1123	tcp
murray	1123	udp
xcompute	11235	tcp
xcompute	11235	sctp
hpvmcontrol	1124	tcp
hpvmcontrol	1124	udp
hpvmagent	1125	tcp
hpvmagent	1125	udp
hpvmdata	1126	tcp
hpvmdata	1126	udp
kwdb-commn	1127	tcp

- بخش **capture file comments** : این بخش برای ضبط کامنت هر فایل می باشد

Hosts	Ports	Capture File Comments
<pre># Resolved addresses found in [no file]  # Comments # # No entries.</pre>		

## سوال ۲ -

به صورت زیر خواهد بود :

00:60:3e	Cisco
00:10:79	Cisco
00:07:0d	Cisco
00:60:09	Cisco
00:90:2b	Cisco
00:60:70	Cisco
00:90:f2	Cisco

## بخش ۲

### سوال ۳ -

با باز کردن این پنجره پروتکل های مختلف که در لایه های گوناگون استفاده شده است را مشاهده خواهیم کرد به صورتی که میتوان متوجه شد که در شنودهایمان چقدر یا چند درصد از هر پروتکلی هست :

Frame	100.0	111526	100.0	73520920	1179 k	0	0	0
Ethernet	100.0	111526	2.1	1561364	25 k	0	0	0
Logical-Link Control	0.3	291	0.0	14374	230	0	0	0
Spanning Tree Protocol	0.2	249	0.0	8715	139	249	8715	139
Dynamic Trunk Protocol	0.0	34	0.0	1088	17	17	544	8
VSS-Monitoring ethernet trailer	0.0	17	0.0	34	0	17	34	0
Cisco Discovery Protocol	0.0	8	0.0	3488	55	8	3488	55
Internet Protocol Version 6	0.2	182	0.0	7280	116	0	0	0
User Datagram Protocol	0.2	169	0.0	1352	21	0	0	0
Simple Service Discovery Protocol	0.0	18	0.0	2124	34	18	2124	34
Multicast Domain Name System	0.1	91	0.0	7566	121	91	7566	121
Link-local Multicast Name Resolution	0.0	8	0.0	246	3	8	246	3
DHCPv6	0.0	52	0.0	4663	74	52	4663	74
Internet Control Message Protocol v6	0.0	13	0.0	256	4	13	256	4
Internet Protocol Version 4	68.5	76351	2.1	1527272	24 k	0	0	0
User Datagram Protocol	2.4	2633	0.0	21064	337	1	8	0
Simple Service Discovery Protocol	1.2	1348	0.3	185948	2982	1348	185948	2982
NetBIOS Name Service	0.1	64	0.0	4170	66	64	4170	66
NetBIOS Datagram Service	0.0	7	0.0	1415	22	0	0	0
SMB (Server Message Block Protocol)	0.0	7	0.0	841	13	0	0	0
SMB MailSlot Protocol	0.0	7	0.0	175	2	0	0	0
Microsoft Windows Browser Protocol	0.0	7	0.0	239	3	7	239	3
Multicast Domain Name System	0.6	700	0.1	44352	711	700	44352	711
Local Service Discovery	0.0	8	0.0	952	15	8	952	15
Link-local Multicast Name Resolution	0.1	82	0.0	2674	42	82	2674	42
Dynamic Host Configuration Protocol	0.0	30	0.0	9038	144	30	9038	144
Domain Name System	0.1	156	0.0	10197	163	156	10197	163
Data	0.2	237	0.4	270478	4338	237	270478	4338
Transmission Control Protocol	66.0	73634	92.8	68233846	1094 k	57052	49128807	788 k
Transport Layer Security	15.1	16810	87.3	64198611	1029 k	16048	53756711	862 k
Malformed Packet	0.1	95	0.0	0	0	95	0	0
Hypertext Transfer Protocol	0.0	14	0.0	4623	74	9	2002	32
Online Certificate Status Protocol	0.0	4	0.0	1108	17	4	1544	24
Line-based text data	0.0	1	0.0	175	2	1	175	2
Data	0.4	425	0.3	191520	3072	425	191520	3072
Internet Group Management Protocol	0.1	63	0.0	1120	17	63	1120	17
Internet Control Message Protocol	0.0	21	0.0	2607	41	21	2607	41
Address Resolution Protocol	31.1	34702	1.3	971656	15 k	34702	971656	15 k
Cisco ISL	0.0	17	0.0	442	7	0	0	0

### سوال ۴ -

همانطور که در تصویر بالا مشاهده میشود در ۶۸.۵ موارد بر روی بستر **IPv4** قرار دارند

## بخش ۳

### سوال ۵ -

در این بخش لایه های مختلف شبکه را مشاهده می کنیم که داده های آماری از روی آن قابل استخراج است .

در اصل این اطلاعات **Conversation** های میان دو نقطه مبدا و مقصد را به ما نشان می دهد :

Ethernet • 85											
IPv4 • 146											
IPv6 • 27											
TCP • 173											
UDP • 316											
Address A	Address 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
00:0e:cf:6b:ad:c0d	04:6c:9d:27:9ec2	۲	128	+	0	۲	128	77.351712	349.4462	0	2
00:e0:4c:68:1c:5f	04:6c:9d:27:9ec2	۱	64	+	0	۱	64	205.354573	0.0000	—	—
01:00:0c:00:00:00	28:c7:ce:0d:f6:81	۱۷	1530	+	0	۱۷	1530	16.488758	480.2433	0	25
01:00:0c:00:00:00	28:c7:ce:0d:f6:81	۲۲	6214	+	0	۲۲	6214	16.488573	480.2435	0	103
01:00:5e:00:00:16	98:29:a6:4a:0d:04	۲۲	1952	+	0	۲۲	1952	201.181013	6.9606	0	2243
01:00:5e:00:00:16	ac:22:0b:0f:38:d1	۱۲	794	+	0	۱۲	794	293.148966	3.8913	0	1632
01:00:5e:00:00:16	88:d7:f6:da:02:dc	۵	300	+	0	۵	300	334.694060	0.4075	0	5890
01:00:5e:00:00:16	80:3f:5d:0d:fc:d5	۱۲	792	+	0	۱۲	792	391.690611	99.8059	0	63
01:00:5e:00:00:16	88:d7:f6:da:02:dc	۸	1003	+	0	۸	1003	25.447721	309.5413	0	25
01:00:5e:00:00:16	20:1a:06:93:c9:58	۵۲۲	52 k	+	0	۵۲۲	52 k	67.593506	431.1013	0	972
01:00:5e:00:00:16	54:ab:3a:b2:f2:06	۱۲	1788	+	0	۱۲	1788	98.700704	86.3358	0	165
01:00:5e:00:00:16	78:24:af:b0:01:89	۲۲	4426	+	0	۲۲	4426	158.358360	305.1229	0	116
01:00:5e:00:00:16	04:d4:c4:75:d5:a4	۸	800	+	0	۸	800	188.565122	2.0698	0	3092
01:00:5e:00:00:16	98:29:a6:4a:0d:04	۵۲	5478	+	0	۵۲	5478	201.184159	160.4136	0	273
01:00:5e:00:00:16	78:24:af:b0:0d:73	۲	714	+	0	۲	714	240.252107	3.0002	0	1903
01:00:5e:00:00:16	ac:22:0b:0f:38:d1	۲۲	5152	+	0	۲۲	5152	294.568961	68.6143	0	600
01:00:5e:00:00:16	80:3f:5d:0d:fc:d5	۲۲	1876	+	0	۲۲	1876	391.835363	105.4799	0	142
01:00:5e:00:00:16	20:1a:06:93:c9:58	۲۲	2376	+	0	۲۲	2376	67.619349	419.2296	0	45
01:00:5e:00:00:16	04:d4:c4:75:d5:a4	۲	150	+	0	۲	150	188.575358	2.0550	0	583
01:00:5e:00:00:16	98:29:a6:4a:0d:04	۲۲	2938	+	0	۲۲	2938	219.123527	235.4680	0	99
01:00:5e:00:00:16	ac:22:0b:0f:38:d1	۲	225	+	0	۲	225	293.163250	3.4270	0	525
01:00:5e:00:00:16	88:d7:f6:da:02:dc	۱	75	+	0	۱	75	334.741026	0.0000	—	—
01:00:5e:00:00:16	80:3f:5d:0d:fc:d5	۲	132	+	0	۲	132	391.851348	99.4138	0	10
01:00:5e:40:98:8f	ac:22:0b:0f:38:d1	۸	1288	+	0	۸	1288	134.433421	305.0096	0	33
01:00:5e:7f:ff:fa	20:1a:06:93:c9:58	۱,۱۱۷	320 k	+	0	۱,۱۱۷	320 k	0.000000	494.5244	0	5185
01:00:5e:7f:ff:fa	78:24:af:b0:01:89	۴۰	7618	+	0	۴۰	7618	2.611017	452.1725	0	134
01:00:5e:7f:ff:fa	ac:22:0b:0f:38:d1	۲۲	5208	+	0	۲۲	5208	25.026703	277.1647	0	150

## بخش ۴

Ethernet · 79		IPv4 · 170		IPv6 · 33		TCP · 331		UDP · 311					
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
13.107.42.16	443	172.23.143.233	50192	1	60	1	60	0	0	28.413085	0.0000	—	—
20.189.173.15	443	172.23.143.233	52959	1	60	1	60	0	0	65.087042	0.0000	—	—
20.189.173.15	443	172.23.143.233	53952	1	60	1	60	0	0	88.120819	0.0000	—	—
40.70.161.7	443	172.23.143.233	53044	4	253	2	145	2	108	3.433638	0.0002	—	—
49.51.129.71	443	172.23.141.101	58068	1	62	1	62	0	0	823.40980	0.0000	—	—
51.137.91.111	443	172.23.143.233	61112	9	492	1	60	8	432	26.167241	43.0681	11	—

## بخش ۵

### سوال ۶ -

در **EndPoints** بر خالف **conversation** که در آن مبدا و مقصد و ارتباط آنها مشخص است ،

فقط اطلاعات مربوط به هر **endpoint** (اطلاعات هر گره) نشان داده شده است :

Ethernet · 35	IPv4 · 150	IPv6 · 20	TCP · 442	UDP · 329	
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets
00:0c:6b:ad:c0:d	133,960	149 M	31,765	3086 k	102,195
01:00:0c:00:00:00	70	6300	0	0	70
01:00:0c:cccc:cc	175	26 k	0	0	175
01:00:5e:00:00:16	98	5830	0	0	98
01:00:5e:00:00:fb	549	50 k	0	0	549
01:00:5e:00:00:fc	26	1772	0	0	26
01:00:5e:40:98:8f	28	4508	0	0	28
01:00:5e:7fff:fa	820	179 k	0	0	820
01:80:c2:00:00:00	1,032	61 k	0	0	1,032
04:6c:9d:27:9e:c2	134,109	149 M	102,467	146 M	31,642
28:c7:ce:0d:f6:a1	1,277	94 k	1,277	94 k	0
28:c7:ce:0d:f6:c0	12	720	12	720	0
2c:56:dc:79:ec:a3	19	2625	19	2625	0
2c:56:dc:79:ec:b8	3	192	0	0	3
33:33:00:00:00:01	2	172	0	0	2
33:33:00:00:00:02	4	272	0	0	4
33:33:00:00:00:0c	217	54 k	0	0	217
33:33:00:00:00:16	10	900	0	0	10

### سوال ۷ -

با توجه به اطلاعات موجود در پنجره های **conversation** و **endpoint** بعضی از مقصد های ارتباط **TCP** سیستم ما بصورت زیر میباشد :

Wireshark · Endpoints · Ethernet

Ethernet · 37	IPv4 · 237	IPv6 · 20	TCP · 826	UDP · 597			
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
172.16.1.227	443	819	793 k	610	771 k	209	
172.16.2.13	443	140	84 k	84	67 k	56	
172.23.141.101	58068	1	62	0	0	1	
172.23.141.101	58559	10	762	0	0	10	
172.23.143.233	63167	38	4604	18	2879	20	
172.23.143.233	56565	26	6185	13	4209	13	
172.23.143.233	56567	49	6330	24	1770	25	
172.23.143.233	56558	219	97 k	80	14 k	139	
172.23.143.233	56569	306	38 k	202	15 k	104	
172.23.143.233	53044	4	253	2	108	2	

Wireshark · Conversations · Ethernet

Ethernet · 82	IPv4 · 262	IPv6 · 33	TCP · 629	UDP · 594		
Address A	Port A	Address B	Port B	Packets	Bytes	Packets
104.208.16.0	443	172.23.143.233	61746	1	60	
108.177.15.188	5228	172.23.141.101	58559	10	762	
172.23.143.233	63167	142.250.185.110	443	38	4604	
172.23.143.233	56565	18.66.112.122	443	26	6185	
172.23.143.233	56567	188.114.96.7	443	49	6330	
172.23.143.233	56558	188.114.97.7	443	219	97 k	
172.23.143.233	56569	20.198.162.78	443	306	38 k	
172.23.143.233	50193	142.250.186.100	443	2,590	2147 k	
172.23.143.233	59927	142.250.185.238	443	981	704 k	
172.23.143.233	59928	142.250.185.238	443	4	264	

////

172.23.143.233	52133	95	10 k	47	5566	48	172.23.143.233	57112	94.182.113.158	443
----------------	-------	----	------	----	------	----	----------------	-------	----------------	-----

////

172.23.143.233	60891	101	66 k	41	10 k	60	172.23.143.233	61379	13.107.42.16	443	93	95 k	24	3945	69	91 k	50.110331	679416	464
----------------	-------	-----	------	----	------	----	----------------	-------	--------------	-----	----	------	----	------	----	------	-----------	--------	-----

## سوال ۸ -

همانطور که مشاهده می شود تعداد تبادلات در این گره خاص بیشتر از بقیه است :

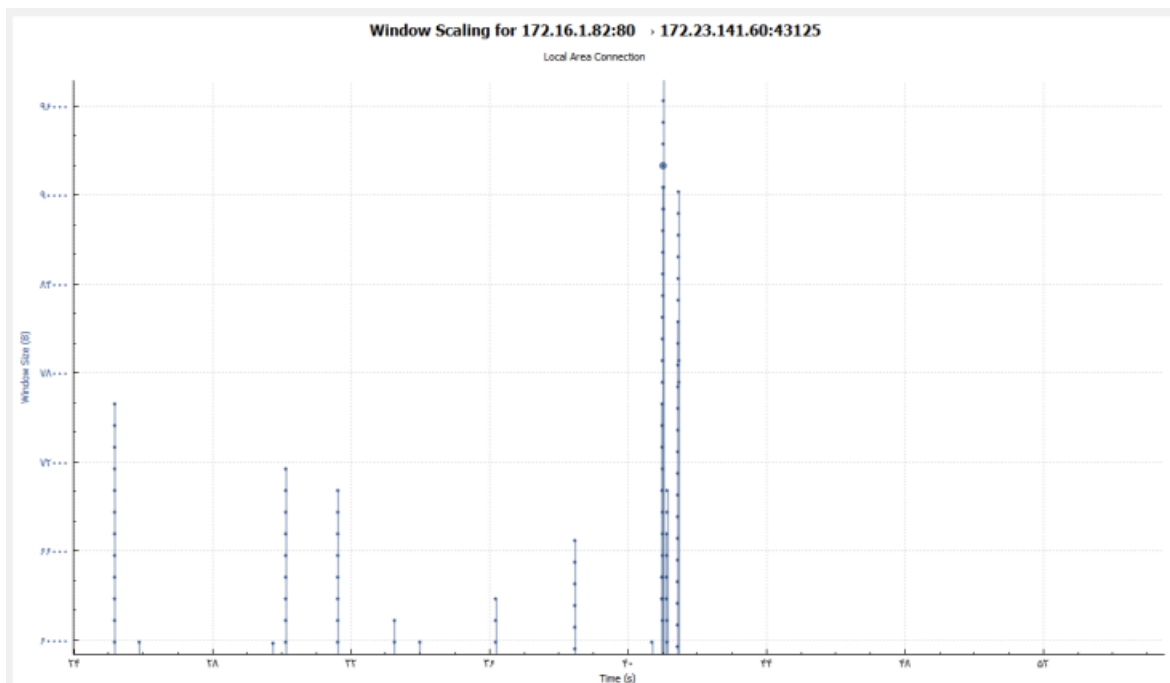
Wireshark - Endpoints - Ethernet							
Ethernet · 40		IPv4 · 245		IPv6 · 22		TCP · 880	
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
94.182.113.158	443	57,866	64 M	42,536	64 M	15,330	

Wireshark - Conversations - Ethernet							
Ethernet · 97		IPv4 · 276		IPv6 · 42		TCP · 683	
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A →	
172.23.143.233	59950	94.182.113.156	443	48,623	64 M	6,2	

## سوال ۹ -

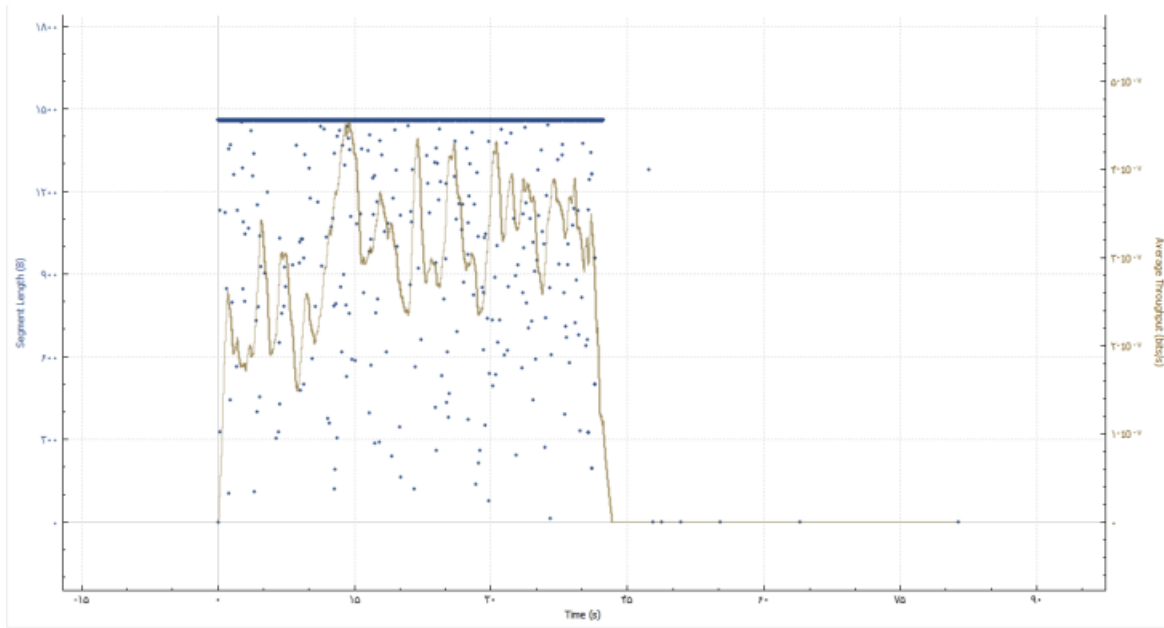
در صورت وجود ازدحام، زمانی را مشخص کردیم که مشاهده می شود **RTT** افزایش پیدا کرده است و **Windows scaling** و **throughput** کاهش پیدا کرده اند .

### Windows Scaling





## Troughput



## Round Trip Time

