

به نام خداوند بخشندۀ مهربان

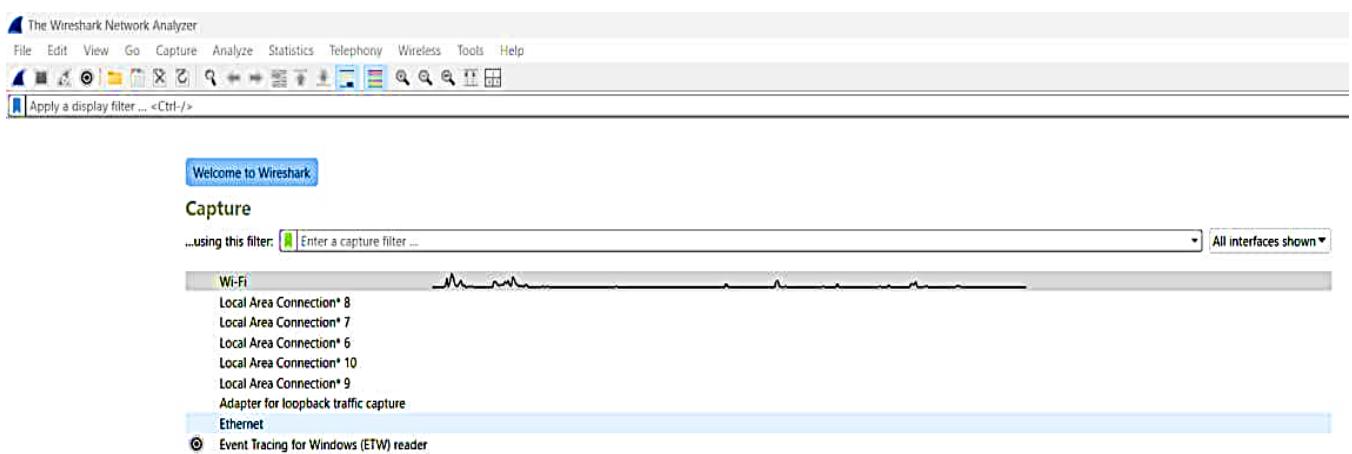
Computer Network

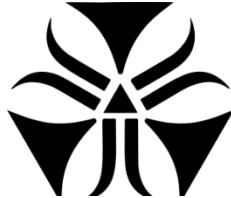
استاد : دکتر رجبی

امیرعلی سهربابی
۴۰۱۱۳۰۴۴۳محمد صالح سهربابی
۴۰۱۱۳۰۴۴۳

تحلیل ترافیک کپچر شده وبسایت طارق(رصدخانه ابن صلاح همدانی)

در اینجا ما وبسایت، صدخانه ابن صلاح همدانی که آدرس url آن هست www.tariq86.ir، با استفاده از نرم افزار **wireshark**، ترافیک کپچر شده آن را تحلیل کردیم.





وقتی که وارد سایت شدیم، packet های زیادی توسط نرم افزار کپچر شدند که بخشی از آنها مطابق شکل زیر است که از پروتکل های مختلف تشکیل شده اند. تا قبل از توقف کپچر کردن، ۶۵ تا پکت ثبت شد.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
3	0.208566	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
5	0.1922058	2.23.169.63	192.168.73.208	SSL	1262	[TCP Previous segment not captured], Continuation Data
7	1.328620	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
9	2.250292	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
13	3.274247	2.23.169.63	192.168.73.208	SSL	1262	[TCP Previous segment not captured], Continuation Data
17	4.092662	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
19	4.400659	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
23	6.626341	2.23.169.63	192.168.73.208	SSL	1262	[TCP Previous segment not captured], Continuation Data
25	6.858335	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
31	7.984872	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
33	8.190141	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
38	8.793485	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
43	9.025566	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
49	9.315589	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
63	9.595371	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data
65	9.931498	2.23.169.63	192.168.73.208	SSL	1262	Continuation Data

[TCP Segment Len: 1208]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1636139568
[Next Sequence Number: 1209 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3540698877
Header Length: 20 bytes (5)
> Flags: 0x10 (ACK)
Window: 501
[Calculated window size: 501]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xb5b1 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (1208 bytes)
Transport Layer Security

Packets: 65 - Dropped: 0 (0.0%)

trafیک شبکه معمولاً شامل تعداد زیادی از بسته ها هست که ممکن است که همه آنها برای ما مفید نباشند. به همین دلیل از سیستم فیلتر استفاده من کنیم...

0100 = Version: 4
0000 0101 = Header Length: 20 bytes (5)
08566	> Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)
J2058	Total Length: 1248
28620	Identification: 0x7be1 (31713)
50292	> 010. = Flags: 0x2, Don't fragment
742470 0000 0000 0000 = Fragment Offset: 0
92626	Time to Live: 54
00659	Protocol: TCP (6)
26341	Header Checksum: 0x0e68 [validation disabled]
58335	[Header checksum status: Unverified]
84872	Source Address: 2.23.169.63
90141	Destination Address: 192.168.73.208
93485?..1 ..hx..E:
25566	0010 04 e0 7b e1 40 00 36 06 0e 68 02 17 a9 3f c0 a8 ..{ @ 6 ..h ..?..
15589	0020 49 d0 01 b1 c3 d2 61 85 82 30 d3 0a c6 fd 50 10 I....a ..0 ..P..
95371	0030 01 f5 8b 51 00 00 4e 49 36 87 7e 9d e7 99 49 0f ..Q..NI 6~..I..
31498	0040 e9 14 eb 81 9e 4d 24 76 36 c3 3f 50 d4 a3 7e 3b ..M\$v 6..?P..~
.....?..1 ..hx..E:	
0050 91 87 1f 34 a5 77 4c 70 9d 80 a3 f6 f5 84 e6 f2 ..4 wlp ..	
0060 b0 cc 17 28 5f bb 1e 85 c3 cc ca f0 0e a4 69 1f ..{ ..-..i..	
0070 20 39 66 22 5d b1 89 95 e6 7a 48 4f 8e 3a c0 6f ..9F]... zH0 ..o	
0080 4b 1e 7f dd dc f7 03 a4 9d fd a9 9e 6d 31 28 55 K....	
0090 dc de 96 34 cc 2b f3 4b a3 d1 fd c9 24 99 4a 89 ..4 + K ... \$..J..	
00a0 0f 53 85 86 5a f7 19 71 04 f8 1b a3 b1 54 4b be ..S..Z..q ..TK..	
00b0 25 0b 97 53 46 a0 af 45 01 52 9b 26 8d 99 4a 5d %..SF..E..R..&..]	
00c0 7d 10 34 51 6c 8d ac 74 d0 fb a8 78 f4 a4 38 71)401..t ..x..8q	
00d0 79 3c 6d 86 4b 95 92 dc 1e e2 ed f3 7f ce f1 86 ysm K... ..	
00e0 ac 46 7d 88 17 14 93 cf db d9 12 7c 59 6c 44 8d F.....[VIM..	
00f0 76 38 ee c8 18 58 b6 1a 5c d8 77 d9 38 40 81 af v8..X.. \w 88..	
0100 e5 db a1 c2 07 f1 ad be 01 68 bd 81 cc 88 5f ..h..	
0110 cf 5e 6a 60 01 5d 36 2e 11 59 64 6d 31 28 de 55 .aj..]6.. .Ydm1(U	