Marek Aleksander, Roman Odarchenko, Sergiy Gnatyuk, Tadeusz Kantor

Basic characteristics of networks with self-similar traffic simulation

JEL: L62 DOI: 10.24136/atest.2019.023
Data zgłoszenia: 15.12.2018 Data akceptacji: 08.02.2019

This paper is devoted to simulations the networks with self-similar traffic. The self-similarity in the stochastic process is identified by calculation of the Herst parameter value. Based on the results, received from the experimental research of network perfomance, we may conclude that the observed traffic in real-time mode is self-similar by its nature. Given results may be used for the further investigation of network traffic and work on the existing models of network traffic (particularly for new networks concepts like IoT, WSN, BYOD etc) from viewpoint of its cybersecurity. Furthermore, the adequacy of the description of real is achieved by complexifying the models, combining several models and integration of new parameters. Accordingly, for more complex models, there are higher computing abilities needed or longer time for the generation of traffic realization.

Keywords: traffic, network traffic models, fractal Brownian motion, self-similiarity, RMD-alhorythm.

Admission

The software tool Wireshark (earlier Ethereal) will be used in order to perform an experimental research of network performance. This is a tool for Ethernet packets analyzing and other networks (sniffer) with open source. The tool has a user graphic interface. The functionality, that is available with Wireshark, is very similar to the abilities of tcpdump tool, however the Wireshark has a praphic user interface and much more possibilities of sorting and filtering of information. The tool allows user to review all the traffic that flows in the network in the real-time mode, transferring it to a network map in promiscuous mode We consider the case of wireless network connection. For the experimental research, we use the network, the scheme of which is illustrated below:

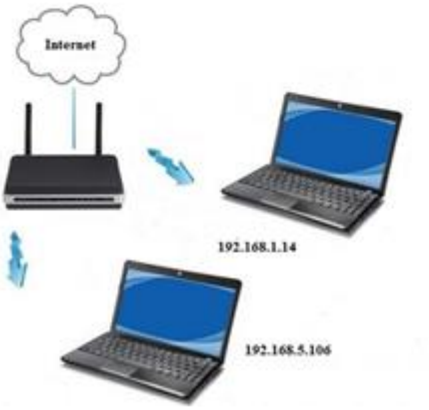
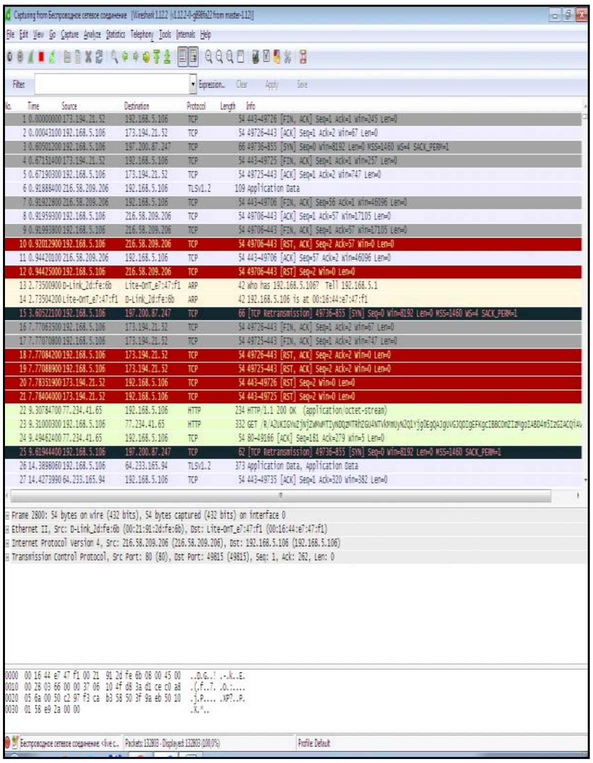


Fig. 1. The scheme of an experimental research network

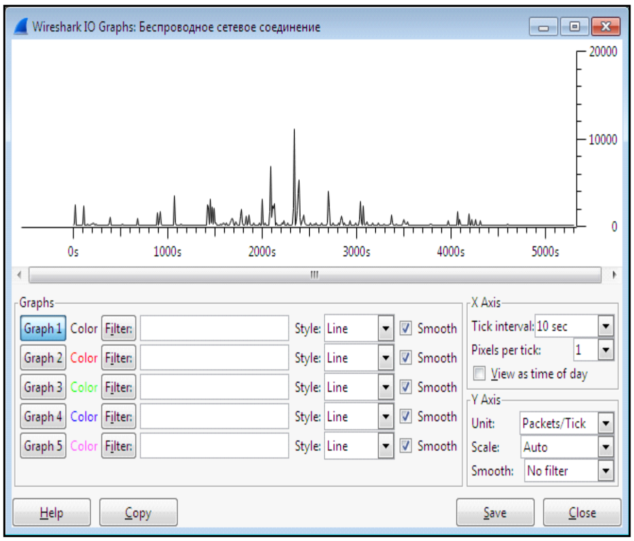
The results of packets interception in the wireless network connection are displayed as:


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
Capturing from Беспроводное сетевое соединение [Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)]

No.  Time       Source             Destination        Protocol  Length  Info
 1 0.00000000 173.194.21.52      192.168.5.106      TCP       54 443→49726 [FIN, ACK] Seq=1 Ack=1 Win=245 Len=0
 2 0.00043100 192.168.5.106      173.194.21.52      TCP       54 49726→443 [ACK] Seq=1 Ack=2 Win=67 Len=0
 3 0.60501200 192.168.5.106      197.200.87.247     TCP       66 49736→855 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 4 0.67151400 173.194.21.52      192.168.5.106      TCP       54 443→49725 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
 5 0.67190300 192.168.5.106      173.194.21.52      TCP       54 49725→443 [ACK] Seq=1 Ack=2 Win=747 Len=0
 6 0.91888400 216.58.209.206     192.168.5.106      TLSv1.2  109 Application Data
 7 0.91922800 216.58.209.206     192.168.5.106      TCP       54 443→49706 [FIN, ACK] Seq=56 Ack=1 Win=46096 Len=0
 8 0.91959300 192.168.5.106      216.58.209.206     TCP       54 49706→443 [ACK] Seq=1 Ack=57 Win=17105 Len=0
 9 0.91993800 192.168.5.106      216.58.209.206     TCP       54 49706→443 [FIN, ACK] Seq=1 Ack=57 Win=17105 Len=0
10 0.92012900 192.168.5.106      216.58.209.206     TCP       54 49706→443 [RST, ACK] Seq=2 Ack=57 Win=0 Len=0
11 0.94420100 216.58.209.206     192.168.5.106      TCP       54 443→49706 [ACK] Seq=57 Ack=2 Win=46096 Len=0
12 0.94425000 192.168.5.106      216.58.209.206     TCP       54 49706→443 [RST] Seq=2 Win=0 Len=0
13 2.73500900 D-Link_2d:fe:6b    Lite-OnT_e7:47:f1  ARP       42 Who has 192.168.5.106?  Tell 192.168.5.1
14 2.73504200 Lite-OnT_e7:47:f1  D-Link_2d:fe:6b    ARP       42 192.168.5.106 is at 00:16:44:e7:47:f1
15 3.60522100 192.168.5.106      197.200.87.247     TCP       66 [TCP Retransmission] 49736→855 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16 7.77063500 192.168.5.106      173.194.21.52      TCP       54 49726→443 [FIN, ACK] Seq=1 Ack=2 Win=67 Len=0
17 7.77070800 192.168.5.106      173.194.21.52      TCP       54 49725→443 [FIN, ACK] Seq=1 Ack=2 Win=747 Len=0
18 7.77084200 192.168.5.106      173.194.21.52      TCP       54 49726→443 [RST, ACK] Seq=2 Ack=2 Win=0 Len=0
19 7.77088900 192.168.5.106      173.194.21.52      TCP       54 49725→443 [RST, ACK] Seq=2 Ack=2 Win=0 Len=0
20 7.78351900 173.194.21.52      192.168.5.106      TCP       54 443→49726 [RST] Seq=2 Win=0 Len=0
21 7.78404000 173.194.21.52      192.168.5.106      TCP       54 443→49725 [RST] Seq=2 Win=0 Len=0
22 9.30784700 77.234.41.65       192.168.5.106      HTTP     234 HTTP/1.1 200 OK  (application/octet-stream)
23 9.31000300 192.168.5.106      77.234.41.65       HTTP     332 GET /R/A2UKIGYwZjNjZwMwMTIyNDQzMTRhZGU4NTVkMmUyN2Q1YjgDEgQAJgUVGJQDIgEFKgcIBBCOmZIzMgoIABD4m5IzGIACQiAv
24 9.49462400 77.234.41.65       192.168.5.106      TCP       54 80→49166 [ACK] Seq=181 Ack=279 Win=5 Len=0
25 9.61944400 192.168.5.106      197.200.87.247     TCP       62 [TCP Retransmission] 49736→855 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
26 14.3898060 192.168.5.106      64.233.165.94      TLSv1.2  373 Application Data, Application Data
27 14.4273990 64.233.165.94      192.168.5.106      TCP       54 443→49735 [ACK] Seq=1 Ack=320 Win=382 Len=0

⊞ Frame 2800: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: D-Link_2d:fe:6b (00:21:91:2d:fe:6b), Dst: Lite-OnT_e7:47:f1 (00:16:44:e7:47:f1)
⊞ Internet Protocol Version 4, Src: 216.58.209.206 (216.58.209.206), Dst: 192.168.5.106 (192.168.5.106)
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49815 (49815), Seq: 1, Ack: 262, Len: 0

0000  00 16 44 e7 47 f1 00 21  91 2d fe 6b 08 00 45 00   ..D.G..! .-.k..E.
0010  00 28 03 66 00 00 37 06  10 4f d8 3a d1 ce c0 a8   .(.f..7. .O.:....
0020  05 6a 00 50 c2 97 f3 ca  b3 58 50 3f 9a eb 50 10   .j.P.... .XP?..P.
0030  01 58 e9 2a 00 00                                  .X.*..

Беспроводное сетевое соединение: <live c...   Packets: 132803 · Displayed: 132803 (100,0%)   Profile: Default
```

Fig. 2. Intercepted packets

It is possible to receive the graphical illustration of intercepted traffic for certain timeframe with the help of tool features, for instance:



Graphs

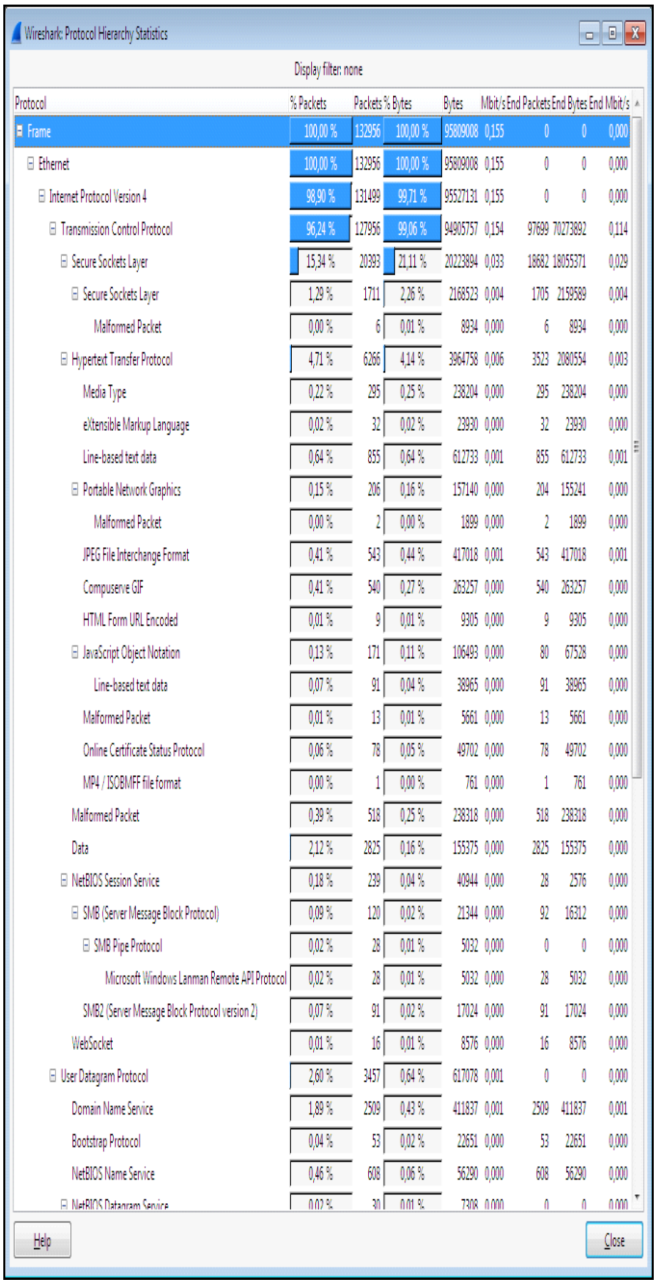
Graph 1	Color	Filter:	Style: Line	☑ Smooth
Graph 2	Color	Filter:	Style: Line	☑ Smooth
Graph 3	Color	Filter:	Style: Line	☑ Smooth
Graph 4	Color	Filter:	Style: Line	☑ Smooth
Graph 5	Color	Filter:	Style: Line	☑ Smooth

X Axis
Tick interval: 10 sec
Pixels per tick: 1
□ View as time of day

Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter

Fig. 3. The graphic illustration of intercepted traffic

There is a possibility of analyzing the percentage of different protocols after analysis of received data. The following steps are needed to get the access to hierarchical statystics: Launching the Wireshark → Wireless network connection → Start → Statistics → Protocol Hierarchy.



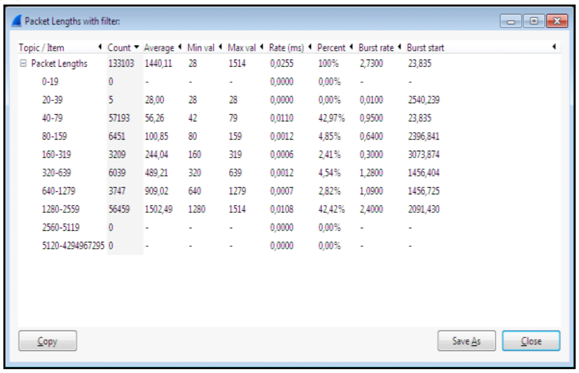
Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100,00 %	132956	100,00 %	95809008	0,155	0	0	0,000
⊟ Ethernet	100,00 %	132956	100,00 %	95809008	0,155	0	0	0,000
⊟ Internet Protocol Version 4	98,90 %	131499	99,71 %	95527131	0,155	0	0	0,000
⊟ Transmission Control Protocol	96,24 %	127956	99,06 %	94905757	0,154	97699	70273892	0,114
⊟ Secure Sockets Layer	15,34 %	20393	21,11 %	20223894	0,033	18682	18055371	0,029
⊟ Secure Sockets Layer	1,29 %	1711	2,26 %	2168523	0,004	1705	2159589	0,004
Malformed Packet	0,00 %	6	0,01 %	8934	0,000	6	8934	0,000
⊟ Hypertext Transfer Protocol	4,71 %	6266	4,14 %	3964758	0,006	3523	2080554	0,003
Media Type	0,22 %	295	0,25 %	238204	0,000	295	238204	0,000
eXtensible Markup Language	0,02 %	32	0,02 %	23930	0,000	32	23930	0,000
Line-based text data	0,64 %	855	0,64 %	612733	0,001	855	612733	0,001
⊟ Portable Network Graphics	0,15 %	206	0,16 %	157140	0,000	204	155241	0,000
Malformed Packet	0,00 %	2	0,00 %	1899	0,000	2	1899	0,000
JPEG File Interchange Format	0,41 %	543	0,44 %	417018	0,001	543	417018	0,001
Compuserve GIF	0,41 %	540	0,27 %	263257	0,000	540	263257	0,000
HTML Form URL Encoded	0,01 %	9	0,01 %	9305	0,000	9	9305	0,000
⊟ JavaScript Object Notation	0,13 %	171	0,11 %	106493	0,000	80	67528	0,000
Line-based text data	0,07 %	91	0,04 %	38965	0,000	91	38965	0,000
Malformed Packet	0,01 %	13	0,01 %	5661	0,000	13	5661	0,000
Online Certificate Status Protocol	0,06 %	78	0,05 %	49702	0,000	78	49702	0,000
MP4 / ISOBMFF file format	0,00 %	1	0,00 %	761	0,000	1	761	0,000
Malformed Packet	0,39 %	518	0,25 %	238318	0,000	518	238318	0,000
Data	2,12 %	2825	0,16 %	155375	0,000	2825	155375	0,000
⊟ NetBIOS Session Service	0,18 %	239	0,04 %	40944	0,000	28	2576	0,000
⊟ SMB (Server Message Block Protocol)	0,09 %	120	0,02 %	21344	0,000	92	16312	0,000
⊟ SMB Pipe Protocol	0,02 %	28	0,01 %	5032	0,000	0	0	0,000
Microsoft Windows Lanman Remote API Protocol	0,02 %	28	0,01 %	5032	0,000	28	5032	0,000
SMB2 (Server Message Block Protocol version 2)	0,07 %	91	0,02 %	17024	0,000	91	17024	0,000
WebSocket	0,01 %	16	0,01 %	8576	0,000	16	8576	0,000
⊟ User Datagram Protocol	2,60 %	3457	0,64 %	617078	0,001	0	0	0,000
Domain Name Service	1,89 %	2509	0,43 %	411837	0,001	2509	411837	0,001
Bootstrap Protocol	0,04 %	53	0,02 %	22651	0,000	53	22651	0,000
NetBIOS Name Service	0,46 %	608	0,06 %	56290	0,000	608	56290	0,000
⊟ NetBIOS Datagram Service	0,02 %	30	0,01 %	7308	0,000	0	0	0,000

Fig. 4. Hierarchy of protocols

With the help of a packet length filter (Lauching Wireshark → Wireless network connection → Start → Statistics → Packet Lengths) we receive the quantity of packets of various duration, their percentage, range of minimum and maximum values of packets etc.

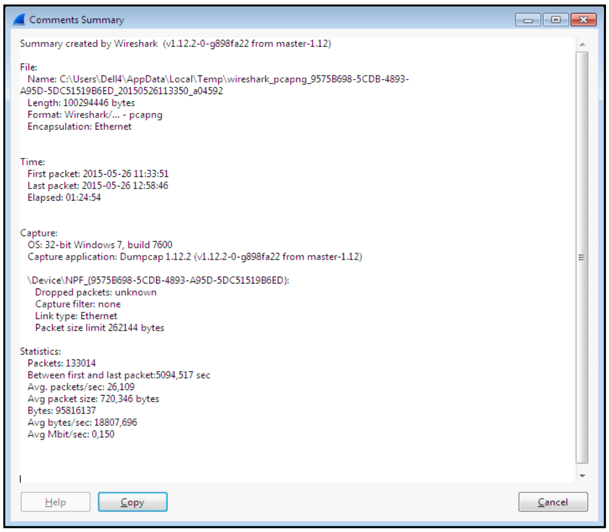


Packet Lengths with filter:

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
⊟ Packet Lengths	133103	1440,11	28	1514	0,0255	100%	2,7300	23,835
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	5	28,00	28	28	0,0000	0,00%	0,0100	2540,239
40-79	57193	56,26	42	79	0,0110	42,97%	0,9500	23,835
80-159	6451	100,85	80	159	0,0012	4,85%	0,6400	2396,841
160-319	3209	244,04	160	319	0,0006	2,41%	0,3000	3073,874
320-639	6039	489,21	320	639	0,0012	4,54%	1,2800	1456,404
640-1279	3747	909,02	640	1279	0,0007	2,82%	1,0900	1456,725
1280-2559	56459	1502,49	1280	1514	0,0108	42,42%	2,4000	2091,430
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120-4294967295	0	-	-	-	0,0000	0,00%	-	-

Fig. 5 The results of packets filtering by length

The general information about the interseption session, meaning its beginning, end, amount of packets, average transmission speed is displayed in Comments Summary.

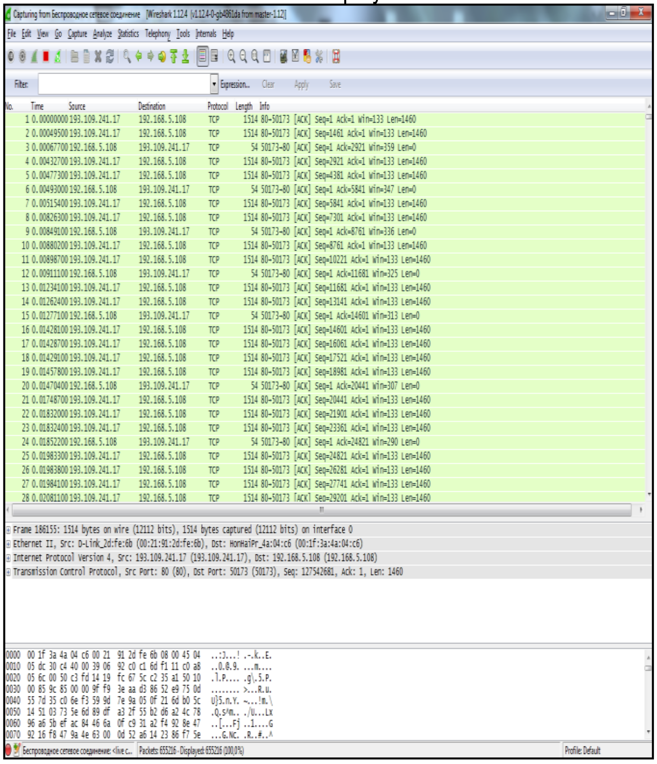


Comments Summary

```
Summary created by Wireshark  (v1.12.2-0-g898fa22 from master-1.12)

File:
  Name: C:\Users\Dell4\AppData\Local\Temp\wireshark_pcapng_9575B698-5CDB-4893-
A95D-5DC51519B6ED_20150526113350_a04592
  Length: 100294446 bytes
  Format: Wireshark/... - pcapng
  Encapsulation: Ethernet


Time:
  First packet: 2015-05-26 11:33:51
  Last packet: 2015-05-26 12:58:46
  Elapsed: 01:24:54


Capture:
  OS: 32-bit Windows 7, build 7600
  Capture application: Dumpcap 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)

  \Device\NPF_{9575B698-5CDB-4893-A95D-5DC51519B6ED}:
    Dropped packets: unknown
    Capture filter: none
    Link type: Ethernet
    Packet size limit 262144 bytes

Statistics:
  Packets: 133014
  Between first and last packet:5094,517 sec
  Avg. packets/sec: 26,109
  Avg packet size: 720,346 bytes
  Bytes: 95816137
  Avg bytes/sec: 18807,696
  Avg Mbit/sec: 0,150
```

Fig. 6. The general information about interception session

Now we consider one more case of traffic interseption in wireless network connection. The results of packets interseption in the wireless network connection are displayed as follows:



Capturing from Беспроводное сетевое соединение   [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.  Time       Source          Destination     Protocol Length Info
   1 0.00000000 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=1 Ack=1 Win=133 Len=1460
   2 0.00049500 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=1461 Ack=1 Win=133 Len=1460
   3 0.00067700 192.168.5.108   193.109.241.17  TCP        54 50173→80 [ACK] Seq=1 Ack=2921 Win=359 Len=0
   4 0.00432700 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=2921 Ack=1 Win=133 Len=1460
   5 0.00477300 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=4381 Ack=1 Win=133 Len=1460
   6 0.00493000 192.168.5.108   193.109.241.17  TCP        54 50173→80 [ACK] Seq=1 Ack=5841 Win=347 Len=0
   7 0.00515400 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=5841 Ack=1 Win=133 Len=1460
   8 0.00826300 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=7301 Ack=1 Win=133 Len=1460
   9 0.00849100 192.168.5.108   193.109.241.17  TCP        54 50173→80 [ACK] Seq=1 Ack=8761 Win=336 Len=0
  10 0.00880200 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=8761 Ack=1 Win=133 Len=1460
  11 0.00898700 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=10221 Ack=1 Win=133 Len=1460
  12 0.00911100 192.168.5.108   193.109.241.17  TCP        54 50173→80 [ACK] Seq=1 Ack=11681 Win=325 Len=0
  13 0.01234100 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=11681 Ack=1 Win=133 Len=1460
  14 0.01262400 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=13141 Ack=1 Win=133 Len=1460
  15 0.01277100 192.168.5.108   193.109.241.17  TCP        54 50173→80 [ACK] Seq=1 Ack=14601 Win=313 Len=0
  16 0.01428100 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=14601 Ack=1 Win=133 Len=1460
  17 0.01428700 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=16061 Ack=1 Win=133 Len=1460
  18 0.01429100 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=17521 Ack=1 Win=133 Len=1460
  19 0.01457800 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=18981 Ack=1 Win=133 Len=1460
  20 0.01470400 192.168.5.108   193.109.241.17  TCP        54 50173→80 [ACK] Seq=1 Ack=20441 Win=307 Len=0
  21 0.01748700 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=20441 Ack=1 Win=133 Len=1460
  22 0.01832000 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=21901 Ack=1 Win=133 Len=1460
  23 0.01832400 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=23361 Ack=1 Win=133 Len=1460
  24 0.01852200 192.168.5.108   193.109.241.17  TCP        54 50173→80 [ACK] Seq=1 Ack=24821 Win=290 Len=0
  25 0.01983300 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=24821 Ack=1 Win=133 Len=1460
  26 0.01983800 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=26281 Ack=1 Win=133 Len=1460
  27 0.01984100 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=27741 Ack=1 Win=133 Len=1460
  28 0.02081100 193.109.241.17  192.168.5.108   TCP      1514 80→50173 [ACK] Seq=29201 Ack=1 Win=133 Len=1460
```

```
⊞ Frame 186155: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
⊞ Ethernet II, Src: D-Link_2d:fe:6b (00:21:91:2d:fe:6b), Dst: HonHaiPr_4a:04:c6 (00:1f:3a:4a:04:c6)
⊞ Internet Protocol Version 4, Src: 193.109.241.17 (193.109.241.17), Dst: 192.168.5.108 (192.168.5.108)
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50173 (50173), Seq: 127542681, Ack: 1, Len: 1460
```

```
0000  00 1f 3a 4a 04 c6 00 21  91 2d fe 6b 08 00 45 04   ..:J...! .-.k..E.
0010  05 dc 30 c4 40 00 39 06  92 c0 c1 6d f1 11 c0 a8   ..0.@.9. ...m....
0020  05 6c 00 50 c3 fd 14 19  fc 67 5c c2 35 a1 50 10   .l.P.... .g\.5.P.
0030  00 85 9c 85 00 00 9f f9  3e aa d3 86 52 e9 75 0d   ........ >...R.u.
0040  55 7d 35 c0 6e f3 59 9d  7e 9a 05 0f 21 6d b0 5c   U}5.n.Y. ~...!m.\
0050  14 51 03 73 5e 6d 89 df  a3 2f 55 b2 d6 a2 4c 78   .Q.s^m.. ./U...Lx
0060  96 a6 5b ef ac 84 46 6a  0f c9 31 a2 f4 92 8e 47   ..[...Fj ..1....G
0070  92 16 f8 47 9a 4e 63 00  0d 52 a6 14 23 86 f7 5e   ...G.Nc. .R..#..^
```

Беспроводное сетевое соединение: <live c... | Packets: 655216 · Displayed: 655216 (100,0%) | Profile: Default

Fig. 7. Intercepted packets

With the help of tool features, it is possible to get the graphical illustration of intersepted traffic for certain timeframe, for instance:

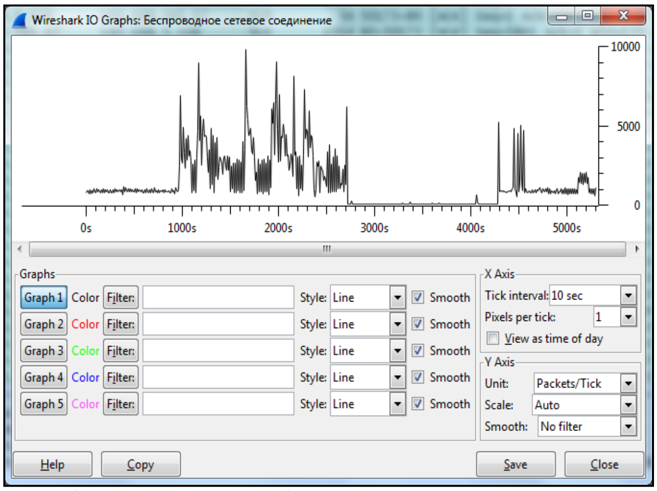
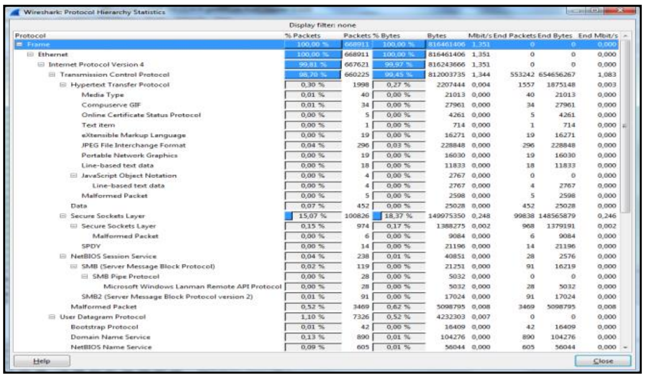


Fig. 8. Graphical illustration of intersepted packets

We now analyze the received data with the help of protocols hierarchy statistics.



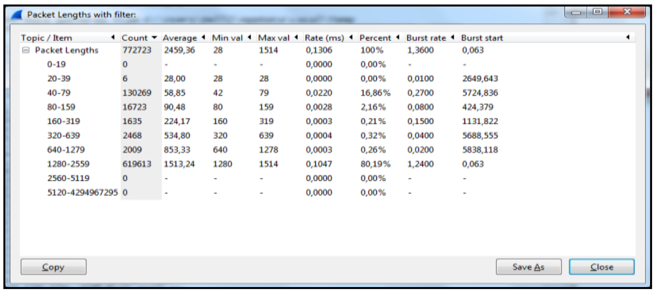
Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	668911	100,00 %	816461406	1,351	0	0	0,000
Ethernet	100,00 %	668911	100,00 %	816461406	1,351	0	0	0,000
Internet Protocol Version 4	99,81 %	667621	99,97 %	816243666	1,351	0	0	0,000
Transmission Control Protocol	98,70 %	660225	99,45 %	812003735	1,344	553242	654656267	1,083
Hypertext Transfer Protocol	0,30 %	1998	0,27 %	2207444	0,004	1557	1875148	0,003
Media Type	0,01 %	40	0,00 %	21013	0,000	40	21013	0,000
Compuserve GIF	0,01 %	34	0,00 %	27961	0,000	34	27961	0,000
Online Certificate Status Protocol	0,00 %	5	0,00 %	4261	0,000	5	4261	0,000
Text item	0,00 %	1	0,00 %	714	0,000	1	714	0,000
eXtensible Markup Language	0,00 %	19	0,00 %	16271	0,000	19	16271	0,000
JPEG File Interchange Format	0,04 %	296	0,03 %	228848	0,000	296	228848	0,000
Portable Network Graphics	0,00 %	19	0,00 %	16030	0,000	19	16030	0,000
Line-based text data	0,00 %	18	0,00 %	11833	0,000	18	11833	0,000
JavaScript Object Notation	0,00 %	4	0,00 %	2767	0,000	0	0	0,000
Line-based text data	0,00 %	4	0,00 %	2767	0,000	4	2767	0,000
Malformed Packet	0,00 %	5	0,00 %	2598	0,000	5	2598	0,000
Data	0,07 %	452	0,00 %	25028	0,000	452	25028	0,000
Secure Sockets Layer	15,07 %	100826	18,37 %	149975350	0,248	99838	148565879	0,246
Secure Sockets Layer	0,15 %	974	0,17 %	1388275	0,002	968	1379191	0,002
Malformed Packet	0,00 %	6	0,00 %	9084	0,000	6	9084	0,000
SPDY	0,00 %	14	0,00 %	21196	0,000	14	21196	0,000
NetBIOS Session Service	0,04 %	238	0,01 %	40851	0,000	28	2576	0,000
SMB (Server Message Block Protocol)	0,02 %	119	0,00 %	21251	0,000	91	16219	0,000
SMB Pipe Protocol	0,00 %	28	0,00 %	5032	0,000	0	0	0,000
Microsoft Windows Lanman Remote API Protocol	0,00 %	28	0,00 %	5032	0,000	28	5032	0,000
SMB2 (Server Message Block Protocol version 2)	0,01 %	91	0,00 %	17024	0,000	91	17024	0,000
Malformed Packet	0,52 %	3469	0,62 %	5098795	0,008	3469	5098795	0,008
User Datagram Protocol	1,10 %	7326	0,52 %	4232303	0,007	0	0	0,000
Bootstrap Protocol	0,01 %	42	0,00 %	16409	0,000	42	16409	0,000
Domain Name Service	0,13 %	890	0,01 %	104276	0,000	890	104276	0,000
NetBIOS Name Service	0,09 %	605	0,01 %	56044	0,000	605	56044	0,000

Fig. 9. Protocol hierarchy

With the help of a packet length filter we receive the quantity of packets of various duration, their percentage, range of minimum and maximum values of packets, etc.

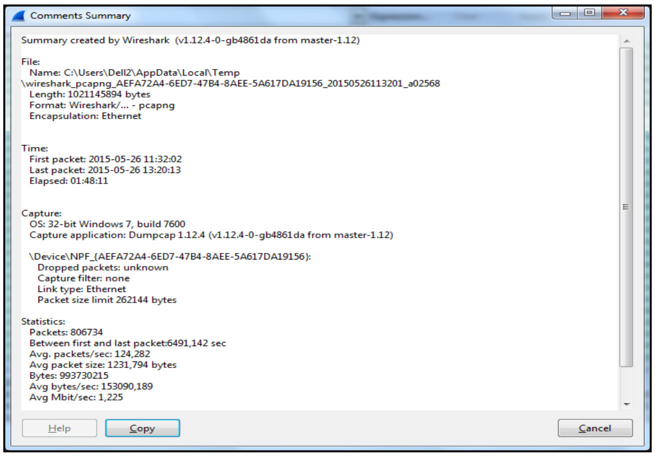


Packet Lengths with filter:

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	772723	2459,36	28	1514	0,1306	100%	1,3600	0,063
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	6	28,00	28	28	0,0000	0,00%	0,0100	2649,643
40-79	130269	58,85	42	79	0,0220	16,86%	0,2700	5724,836
80-159	16723	90,48	80	159	0,0028	2,16%	0,0800	424,379
160-319	1635	224,17	160	319	0,0003	0,21%	0,1500	1131,822
320-639	2468	534,80	320	639	0,0004	0,32%	0,0400	5688,555
640-1279	2009	853,33	640	1278	0,0003	0,26%	0,0200	5838,118
1280-2559	619613	1513,24	1280	1514	0,1047	80,19%	1,2400	0,063
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120-4294967295	0	-	-	-	0,0000	0,00%	-	-

Fig. 10. The results of packets filtering by length

The general information about the interseption session, meaning its beginning, end, amount of packets, average transmission speed is displayed in Comments Summary.

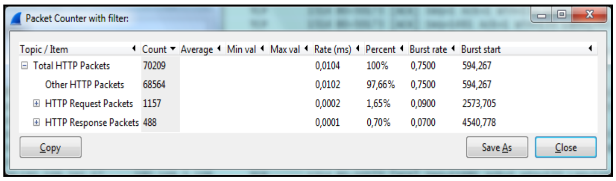


Comments Summary

```
Summary created by Wireshark  (v1.12.4-0-gb4861da from master-1.12)

File:
  Name: C:\Users\Dell2\AppData\Local\Temp
\wireshark_pcapng_AEFA72A4-6ED7-47B4-8AEE-5A617DA19156_20150526113201_a02568
  Length: 1021145894 bytes
  Format: Wireshark/... - pcapng
  Encapsulation: Ethernet


Time:
  First packet: 2015-05-26 11:32:02
  Last packet: 2015-05-26 13:20:13
  Elapsed: 01:48:11


Capture:
  OS: 32-bit Windows 7, build 7600
  Capture application: Dumpcap 1.12.4 (v1.12.4-0-gb4861da from master-1.12)

  \Device\NPF_{AEFA72A4-6ED7-47B4-8AEE-5A617DA19156}:
    Dropped packets: unknown
    Capture filter: none
    Link type: Ethernet
    Packet size limit 262144 bytes

Statistics:
  Packets: 806734
  Between first and last packet:6491,142 sec
  Avg. packets/sec: 124,282
  Avg packet size: 1231,794 bytes
  Bytes: 993730215
  Avg bytes/sec: 153090,189
  Avg Mbit/sec: 1,225
```

Fig. 11. The general information about interception session

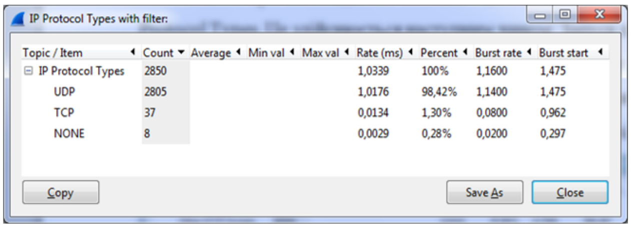
In addition, it is possible to get the quantity of HTTP and IP protocol types, if necessary. It should be done as follows: Lauching Wireshark -> Wireless network connection -> Start -> Statistics -> HTTP -> Packet Counter or Lauching Wireshark -> WWireless network nonnection -> Start -> Statistics -> IP Statistics -> IP Protocol Types accordingly.



Packet Counter with filter:

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total HTTP Packets	70209				0,0104	100%	0,7500	594,267
Other HTTP Packets	68564				0,0102	97,66%	0,7500	594,267
HTTP Request Packets	1157				0,0002	1,65%	0,0900	2573,705
HTTP Response Packets	488				0,0001	0,70%	0,0700	4540,778

Fig. 12. Quantity of HTTP packets

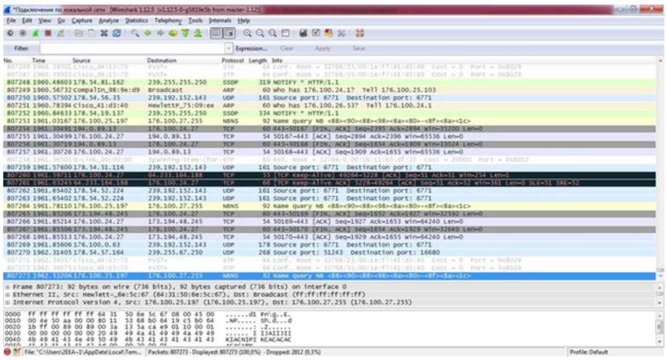


IP Protocol Types with filter:

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
IP Protocol Types	2850				1,0339	100%	1,1600	1,475
UDP	2805				1,0176	98,42%	1,1400	1,475
TCP	37				0,0134	1,30%	0,0800	0,962
NONE	8				0,0029	0,28%	0,0200	0,297

Fig. 13. IP Protocol Types

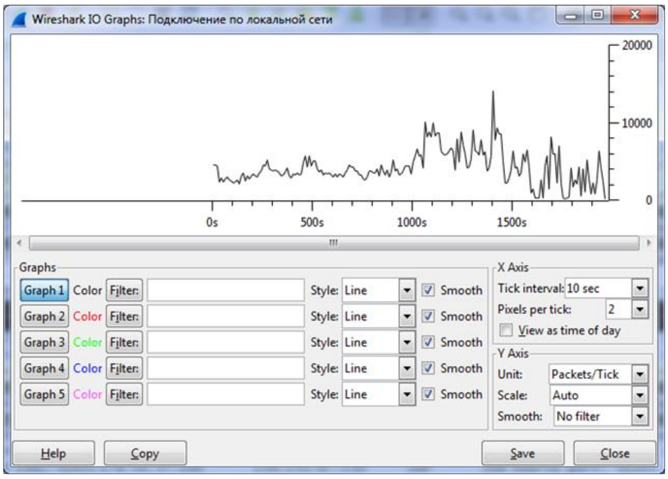
With the help of network interface, we now chosing the connection in a local network and performing the packet interseption in real time mode. This action includes following steps: Launching Wireshark -> Local network connection -> Start. Illustration of intersepted packets:


*Подключение по локальной сети [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.    Time       Source            Destination        Protocol Length Info
807246 1960.39301 Cisco_d4:15:70    PVST+              STP      64 Conf. Root = 32768/23/00:1e:f7:41:d3:40  Cost = 0  Port = 0x8029
807247 1960.39302 Cisco_d4:15:70    PVST+              STP      64 Conf. Root = 32768/33/00:1e:f7:41:d3:40  Cost = 0  Port = 0x8029
807248 1960.48603 178.54.81.162     239.255.255.250    SSDP    319 NOTIFY * HTTP/1.1
807249 1960.56732 CompalIn_98:9e:d9 Broadcast          ARP      60 Who has 176.100.24.1?  Tell 176.100.25.103
807250 1960.57502 178.54.56.35      239.192.152.143    UDP     161 Source port: 6771  Destination port: 6771
807251 1960.78394 Cisco_41:d3:40    HewlettP_75:09:ee  ARP      60 Who has 176.100.26.53?  Tell 176.100.24.1
807252 1960.84633 178.54.19.137     239.255.255.250    SSDP    334 NOTIFY * HTTP/1.1
807253 1961.03167 176.100.25.197    176.100.27.255     NBNS     92 Name query NB <88><90><88><98><8a><80>-<8f><8a><1c>
807254 1961.30491 194.0.89.13       176.100.24.27      TCP      60 443→50167 [FIN, ACK] Seq=2395 Ack=2894 Win=35200 Len=0
807255 1961.30499 176.100.24.27     194.0.89.13        TCP      54 50167→443 [ACK] Seq=2894 Ack=2396 Win=65536 Len=0
807256 1961.30719 194.0.89.13       176.100.24.27      TCP      60 443→50168 [FIN, ACK] Seq=1654 Ack=1909 Win=33024 Len=0
807257 1961.30726 176.100.24.27     194.0.89.13        TCP      54 50168→443 [ACK] Seq=1909 Ack=1655 Win=65536 Len=0
807258 1961.36505 D-Link_00:00:00   Spanning-tree-(for-STP      60 RST. Root = 32768/0/00:1b:11:b5:df:22  Cost = 20000  Port = 0x8012
807259 1961.57600 178.54.51.116     239.192.152.143    UDP     161 Source port: 6771  Destination port: 6771
807260 1961.59711 176.100.24.27     64.233.164.188     TCP      55 [TCP Keep-Alive] 49264→5228 [ACK] Seq=51 Ack=51 Win=254 Len=1
807261 1961.63245 64.233.164.188    176.100.24.27      TCP      66 [TCP Keep-Alive ACK] 5228→49264 [ACK] Seq=51 Ack=52 Win=361 Len=0 SLE=51 SRE=52
807262 1961.65402 178.54.52.224     239.192.152.143    UDP     161 Source port: 6771  Destination port: 6771
807263 1961.65402 178.54.52.224     239.192.152.143    UDP     161 Source port: 6771  Destination port: 6771
807264 1961.78110 176.100.25.197    176.100.27.255     NBNS     92 Name query NB <88><90><88><98><8a><80>-<8f><8a><1c>
807265 1961.85206 173.194.48.245    176.100.24.27      TCP      60 443→50169 [FIN, ACK] Seq=1652 Ack=1927 Win=32592 Len=0
807266 1961.85214 176.100.24.27     173.194.48.245     TCP      54 50169→443 [ACK] Seq=1927 Ack=1653 Win=64240 Len=0
807267 1961.85506 173.194.48.245    176.100.24.27      TCP      60 443→50170 [FIN, ACK] Seq=1654 Ack=1929 Win=32640 Len=0
807268 1961.85513 176.100.24.27     173.194.48.245     TCP      54 50170→443 [ACK] Seq=1929 Ack=1655 Win=64240 Len=0
807269 1961.85606 176.100.0.63      239.192.152.143    UDP     178 Source port: 6771  Destination port: 6771
807270 1962.31405 178.54.57.164     239.255.67.250     UDP     268 Source port: 51243  Destination port: 16680
807271 1962.39257 Cisco_d4:15:70    PVST+              STP      64 Conf. Root = 32768/23/00:1e:f7:41:d3:40  Cost = 0  Port = 0x8029
807272 1962.39275 Cisco_d4:15:70    PVST+              STP      64 Conf. Root = 32768/33/00:1e:f7:41:d3:40  Cost = 0  Port = 0x8029
807273 1962.53206 176.100.25.197    176.100.27.255     NBNS     92 Name query NB <88><90><88><98><8a><80>-<8f><8a><1c>

⊞ Frame 807273: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
⊞ Ethernet II, Src: Hewlett-_6e:5c:67 (64:31:50:6e:5c:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 176.100.25.197 (176.100.25.197), Dst: 176.100.27.255 (176.100.27.255)

0000  ff ff ff ff ff ff 64 31  50 6e 5c 67 08 00 45 00   ......d1 Pn\g..E.
0010  00 4e 50 aa 00 00 80 11  53 68 b0 64 19 c5 b0 64   .NP..... Sh.d...d
0020  1b ff 00 89 00 89 00 3a  13 5a ca e9 01 10 00 01   .......: .Z......
0030  00 00 00 00 00 00 20 49  49 4a 41 49 49 4a 49 49   ...... I IJAIIJII
0040  4b 49 41 43 4e 49 50 49  4b 43 41 43 41 43 41 43   KIACNIPI KCACACAC

File: "C:\Users\2EEA~1\AppData\Local\Tem...  Packets: 807273 · Displayed: 807273 (100,0%) · Dropped: 2812 (0,3%)  Profile: Default
```

Fig. 14. Intersepted packets

With the use of graphic interface (Launching Wireshark -> Local network connection -> Start -> Statistics -> IO Graph), we can observe the graphical illustration of interepted traffic.



Graphs

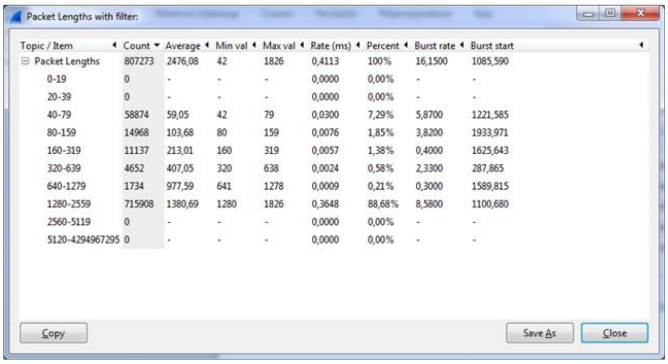
Graph 1	Color	Filter:		Style:	Line	☑ Smooth
Graph 2	Color	Filter:		Style:	Line	☑ Smooth
Graph 3	Color	Filter:		Style:	Line	☑ Smooth
Graph 4	Color	Filter:		Style:	Line	☑ Smooth
Graph 5	Color	Filter:		Style:	Line	☑ Smooth

X Axis
Tick interval: 10 sec
Pixels per tick: 2
□ View as time of day

Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter

Fig. 15. Graphic illustration of intersepted traffic

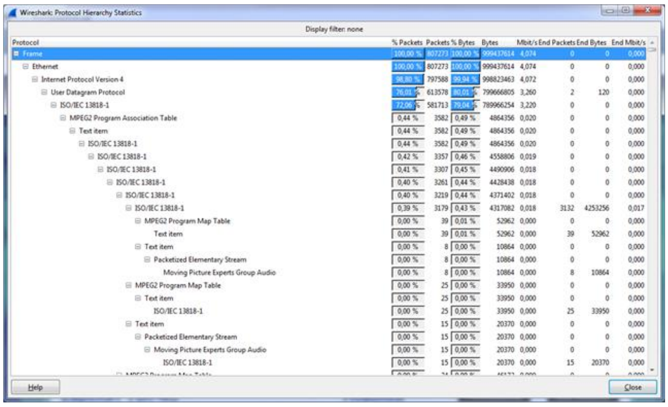
With the help of a packet length filter, we receive the quantity of packets of various duration, their percentage, range of minimum and maximum values of packets, etc.



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
⊟ Packet Lengths	807273	2476,08	42	1826	0,4113	100%	16,1500	1085,590
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	58874	59,05	42	79	0,0300	7,29%	5,8700	1221,585
80-159	14968	103,68	80	159	0,0076	1,85%	3,8200	1933,971
160-319	11137	213,01	160	319	0,0057	1,38%	0,4000	1625,643
320-639	4652	407,05	320	638	0,0024	0,58%	2,3300	287,865
640-1279	1734	977,59	641	1278	0,0009	0,21%	0,3000	1589,815
1280-2559	715908	1380,69	1280	1826	0,3648	88,68%	8,5800	1100,680
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120-4294967295	0	-	-	-	0,0000	0,00%	-	-

Fig. 16. The results of packets filtering by length

There is a possibility of percentage analysis of different protocols after the data alanysis. To access the protocols hierarchy statistics following steps are needed: Launching Wireshark -> Local network connection -> Start -> Statistics -> Protocol Hierarchy.

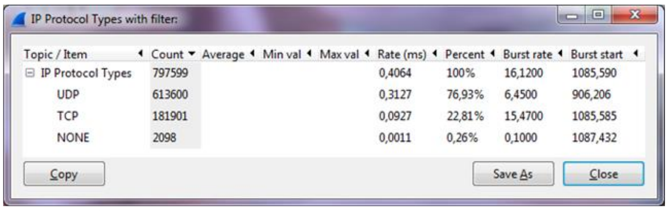


Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100,00 %	807273	100,00 %	999437614	4,074	0	0	0,000
⊟ Ethernet	100,00 %	807273	100,00 %	999437614	4,074	0	0	0,000
⊟ Internet Protocol Version 4	98,80 %	797588	99,94 %	998823463	4,072	0	0	0,000
⊟ User Datagram Protocol	76,01 %	613578	80,01 %	799666805	3,260	2	120	0,000
⊟ ISO/IEC 13818-1	72,06 %	581713	79,04 %	789966254	3,220	0	0	0,000
⊟ MPEG2 Program Association Table	0,44 %	3582	0,49 %	4864356	0,020	0	0	0,000
⊟ Text item	0,44 %	3582	0,49 %	4864356	0,020	0	0	0,000
⊟ ISO/IEC 13818-1	0,44 %	3582	0,49 %	4864356	0,020	0	0	0,000
⊟ ISO/IEC 13818-1	0,42 %	3357	0,46 %	4558806	0,019	0	0	0,000
⊟ ISO/IEC 13818-1	0,41 %	3307	0,45 %	4490906	0,018	0	0	0,000
⊟ ISO/IEC 13818-1	0,40 %	3261	0,44 %	4428438	0,018	0	0	0,000
⊟ ISO/IEC 13818-1	0,40 %	3219	0,44 %	4371402	0,018	0	0	0,000
⊟ ISO/IEC 13818-1	0,39 %	3179	0,43 %	4317082	0,018	3132	4253256	0,017
⊟ MPEG2 Program Map Table	0,00 %	39	0,01 %	52962	0,000	0	0	0,000
Text item	0,00 %	39	0,01 %	52962	0,000	39	52962	0,000
⊟ Text item	0,00 %	8	0,00 %	10864	0,000	0	0	0,000
⊟ Packetized Elementary Stream	0,00 %	8	0,00 %	10864	0,000	0	0	0,000
Moving Picture Experts Group Audio	0,00 %	8	0,00 %	10864	0,000	8	10864	0,000
⊟ MPEG2 Program Map Table	0,00 %	25	0,00 %	33950	0,000	0	0	0,000
⊟ Text item	0,00 %	25	0,00 %	33950	0,000	0	0	0,000
ISO/IEC 13818-1	0,00 %	25	0,00 %	33950	0,000	25	33950	0,000
⊟ Text item	0,00 %	15	0,00 %	20370	0,000	0	0	0,000
⊟ Packetized Elementary Stream	0,00 %	15	0,00 %	20370	0,000	0	0	0,000
⊟ Moving Picture Experts Group Audio	0,00 %	15	0,00 %	20370	0,000	0	0	0,000
ISO/IEC 13818-1	0,00 %	15	0,00 %	20370	0,000	15	20370	0,000

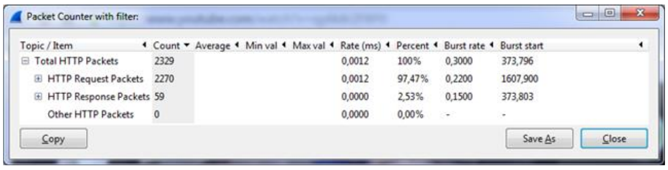
Fig. 17. Protocol hierarchy

In addition, it is possible to get the quantity of HTTP and IP protocol types, if necessary. It should be done as follows: Lauching Wireshark -> Wireless network connection -> Start -> Statistics -> HTTP -> Packet Counter or Lauching Wireshark -> WWireless network nonnection -> Start -> Statistics -> IP Statistics -> IP Protocol Types accordingly.



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
⊟ IP Protocol Types	797599				0,4064	100%	16,1200	1085,590
UDP	613600				0,3127	76,93%	6,4500	906,206
TCP	181901				0,0927	22,81%	15,4700	1085,585
NONE	2098				0,0011	0,26%	0,1000	1087,432

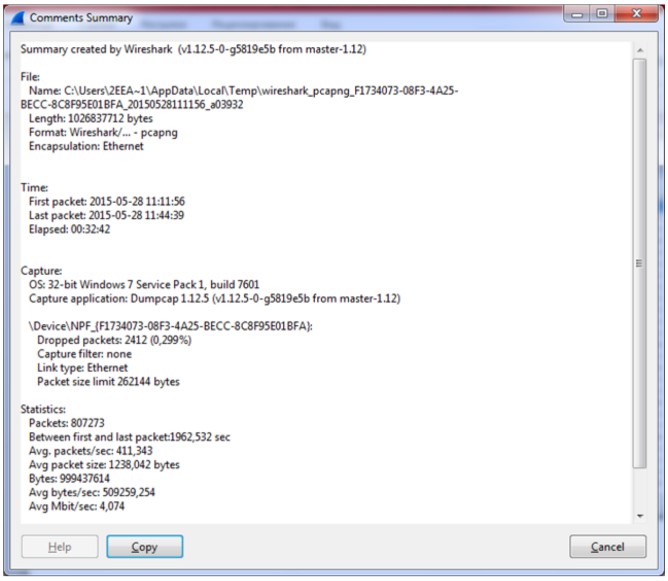
Fig. 18. Quantity of HTTP packets



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
⊟ Total HTTP Packets	2329				0,0012	100%	0,3000	373,796
⊞ HTTP Request Packets	2270				0,0012	97,47%	0,2200	1607,900
⊞ HTTP Response Packets	59				0,0000	2,53%	0,1500	373,803
Other HTTP Packets	0				0,0000	0,00%	-	-

Fig. 19. IP Protocol Types

The general information about the interseption session, meaning its beginning, end, amount of packets, average transmission speed is displayed in Comments Summary.



```
Summary created by Wireshark  (v1.12.5-0-g5819e5b from master-1.12)

File:
  Name: C:\Users\2EEA~1\AppData\Local\Temp\wireshark_pcapng_F1734073-08F3-4A25-
BECC-8C8F95E01BFA_20150528111156_a03932
  Length: 1026837712 bytes
  Format: Wireshark/... - pcapng
  Encapsulation: Ethernet


Time:
  First packet: 2015-05-28 11:11:56
  Last packet: 2015-05-28 11:44:39
  Elapsed: 00:32:42


Capture:
  OS: 32-bit Windows 7 Service Pack 1, build 7601
  Capture application: Dumpcap 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)

  \Device\NPF_{F1734073-08F3-4A25-BECC-8C8F95E01BFA}:
    Dropped packets: 2412 (0,299%)
    Capture filter: none
    Link type: Ethernet
    Packet size limit 262144 bytes

Statistics:
  Packets: 807273
  Between first and last packet:1962,532 sec
  Avg. packets/sec: 411,343
  Avg packet size: 1238,042 bytes
  Bytes: 999437614
  Avg bytes/sec: 509259,254
  Avg Mbit/sec: 4,074
```

Fig. 20. General information about the interseption seanse

We now compare the quantity of intercepted packets for considered cases and performing the graphical illustration.

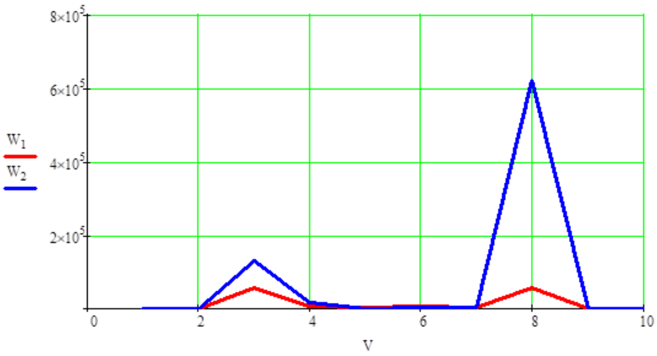


Fig. 21. Compairing the results of filtering packets by length

We now check if the experimentally received flow is self-similar. The Dispersion – time interdependence for the intercepted traffic:

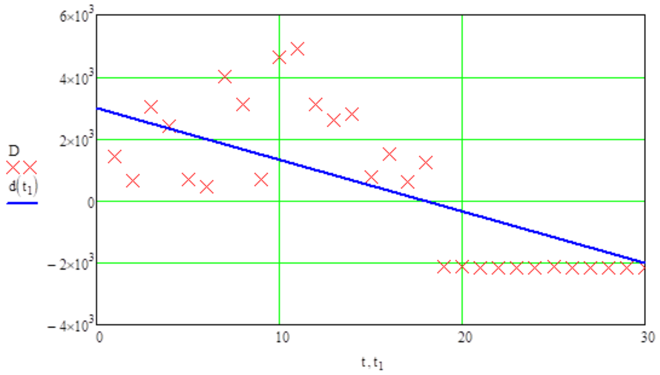


Fig. 22. Dispersion – time interdependence for the intercepted traffic

The reseived slope of line equals . With the help of it we can calculate the self-similarity coefficient $H = 1 - |\beta|$. The resulting scope of line equals 0,1687. It means that the value of Herst parameter is 0,8313, which is equal to value of Herst parameter for the self-similar traffic ($0{,}5 < H < 1$).

Conclusions

Traditionally, the self-similarity in the stochastic process is identified by calculation of the Herst (H) parameter value. The fact, that$0.5 < H < 1$, meaning that Herst parameter is different of 0.5, is an enough reason to state that the process is self-similar. Not to mention, that the value of a Herst parameter which is close to one, may mean that the process is determined, not random: for a gange of strictly-determined processes, structure is strictly repeated on any scale, which leads to “one” value of Herst parameter. Based on the results, that were received from the experimental research of network perfomance, dispersion – time interdependence for the intercepted traffic and the slope of line β, we may conclude that the observed traffic in real-time mode is self-similar by its nature. The results of this paper may be used for the further investigation of network traffic and work on the existing models of network traffic. Furthermore, the adequacy of the description of real is achieved by complexifying the models, combining several models and integration of new parameters. Accordingly, for more complex models, there are higher computing abilities needed or longer time for the generation of traffic realization.

References

1. *O. Sheluhin.* Multifractals. Infocommunicational applications, M.: Hotline-Telecom, 2011, 576 p.
2. *A. Melikov, L. Ponomarenko, V. Paladuk.* Teletraffic: Models, methods, optimization, K.: IPK «Polytechnica», 2007,256 p.
3. *O. Sheluhin, A Tenyakshev, A. Osin.* Modeling of information systems. Study guide, M.: Radiotechnica, 2005, 368 p.
4. *A. Privalov, M. Bayeva.* Modeling of self-simirlar traffic// News from the Samara science centre of Russian science academy, P. 1041-1046.
5. *A. Kostromitskyi.* Approaches to self-similar traffic modeling // Eastern-Europe journal of modern technologies, 2010, 4/7 (46), C. 46-49.
6. *R. Shyhaliyev.* Analysis and classification of network traffic in computer networks // Information technologies problems, 2010. – №2, C. 15-23.
7. *E. Dobrovolskyi, O. Nechyporuk.* Modeling of the network traffic with the use of context methods // Science works ONAZ named after. O. S. Popov, 2005, №1, P. 24-32.
8. *I. Matychyn, V. Onyshchevko.* Modeling and analysis of telecommunication systems and networks traffic // Visnyk DUIKT, 2013, №4, P. 20-27.
9. *N. Trenogyn, D. E. Sokolov.* Fractal features of network traffic in a client-server information system // Vestnyk NII SYVPT, P. 163-172.
10. *A. Kostromitsky* Network traffic analysis and monitoring tool review, Access mode: http://pi.314159.ru/volotka/volotka1.htm
11. *Y. Semenov* Network modeling, Access mode: http://citforum.ck.ua/nets/semenov/4/45/modl4517.shtml

Authors

DSc, PhD, docent **Marek Aleksander** - Institute of Technology, State University of Applied Sciences in Nowy Sącz, e-mail: aleksandermarek4@gmail.com
PhD Associate Professor **Roman Odarchenko** - Academic Dept of Telecommunication Systems, National Aviation University (Kyiv, Ukraine)
DSc, Associate Professor **Sergiy Gnatyuk** - Academic Dept of IT-Security, National Aviation University (Kyiv, Ukraine)
Mr. **Tadeusz Kantor** - Institute of Technology State University of Applied Sciences in Nowy Sącz