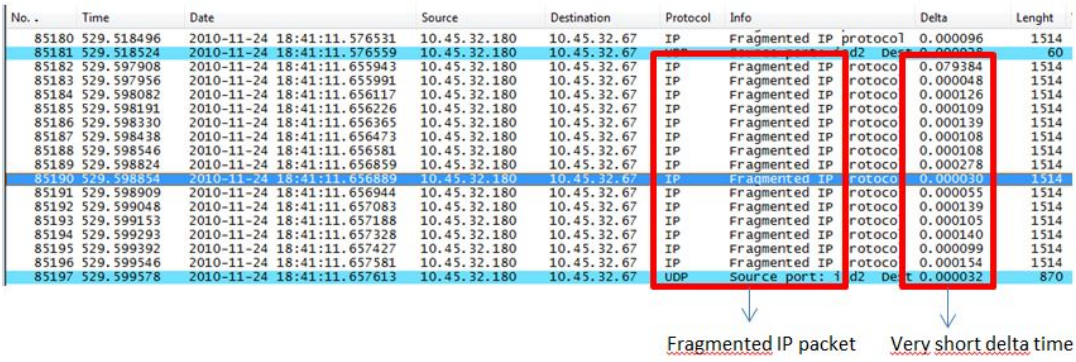
How to identify a burst in a capture ?

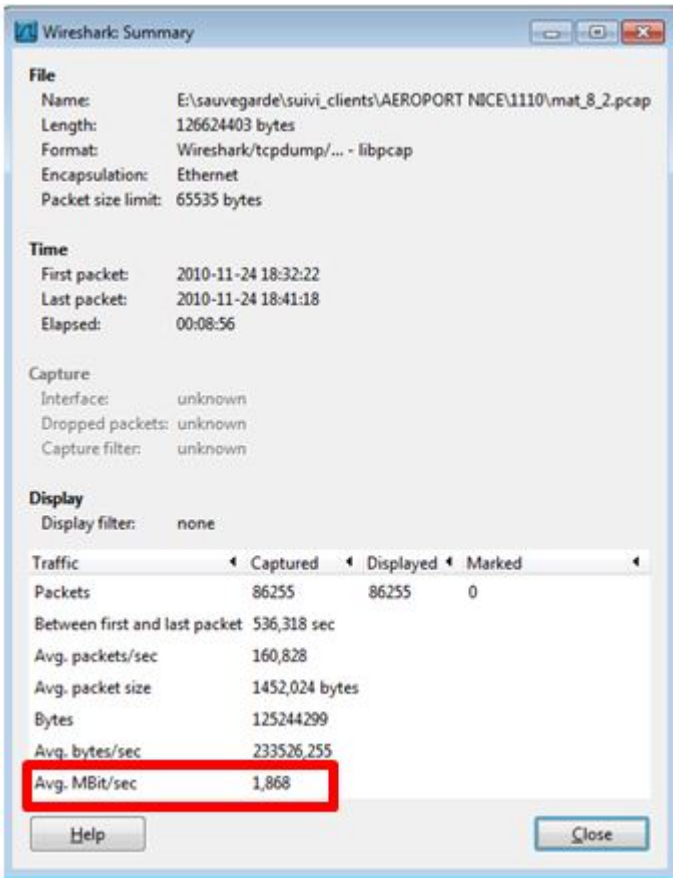
- 2018-02-21 - Wireshark

Bursts beeing sometimes source of problems (mainly in video projects), their identification is important nevertheless the SNMP tools can't help because they just give an average on several seconds while the burst usually lenghts few ms.

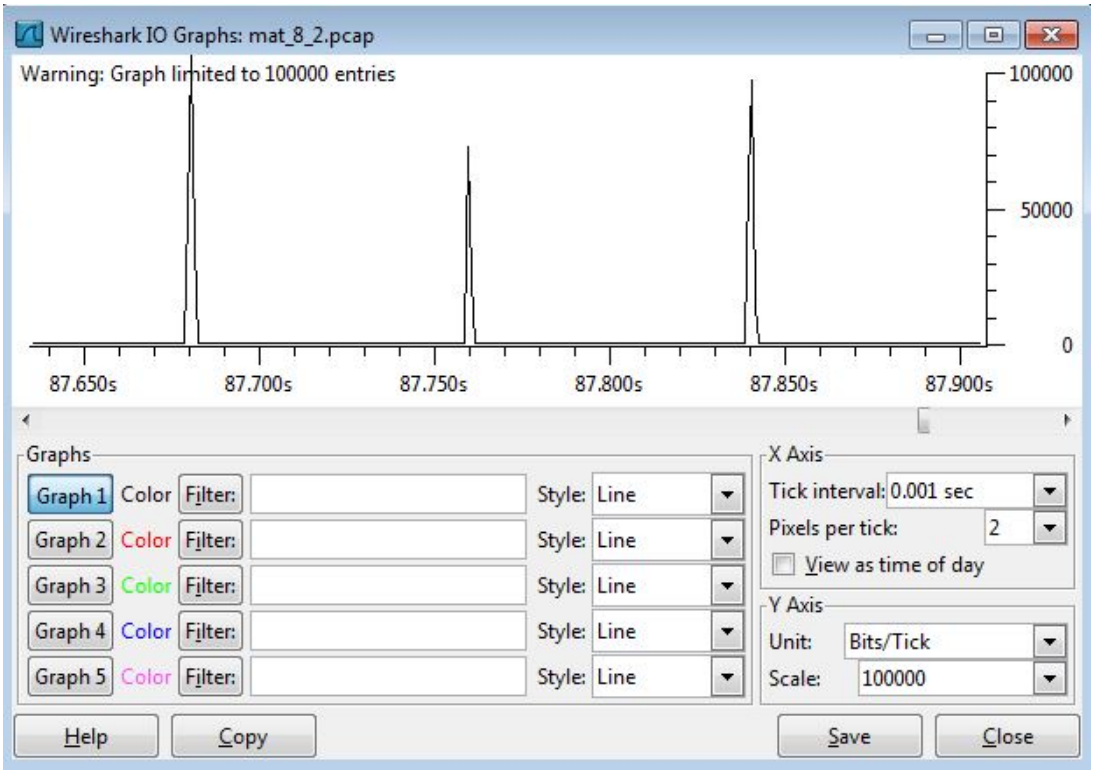
The best way to identify them (using free tool) is to analyse a capture of the stream with Wireshark.
First of all, in the main Window you may find some hints such as ""fragmented IP packets"" which are usually big size IP packets fragmented to be sent on Ethernet. Of course the delay between the fragments is extremely short. Adding the ""Delta time between packets"" in you main view will help you to see that.



Nevertheless the summary of your capture may show a very low load average :



Then go in ""Statistics"", ""IO Graph"", and in the new Window enter the following settings :
X Axis :
Tick interval : 0,001 sec
Y Axis
Units : Bits / Tick
Scale : 100000 (for a capture done on a Fast Ethernet Link)
1000000 (for a capture done on a Gigabit link)
Then the network load will be displayed in precision by the graph knowing the the scale correspond to a range from 0 % to 100 % of the link capacity.
In our example. in spite of a average load less than 2 Mb/s (usual for video streams) , the bursts reach 100 Mb/s, the max link capacity.


Wireshark IO Graphs: mat_8_2.pcap
Warning: Graph limited to 100000 entries
100000
50000
0
87.650s
87.700s
87.750s
87.800s
87.850s
87.900s
Graphs
Graph 1
Color
Filter:
Style:
Line
Graph 2
Color
Filter:
Style:
Line
Graph 3
Color
Filter:
Style:
Line
Graph 4
Color
Filter:
Style:
Line
Graph 5
Color
Filter:
Style:
Line
X Axis
Tick interval:
0.001 sec
Pixels per tick:
2
View as time of day
Y Axis
Unit:
Bits/Tick
Scale:
100000
Help
Copy
Save
Close