

Wissensdatenbank > Tools > Wireshark > How to identify a burst in a capture ?

## 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.

| lo    | Time        | Date                       | Source       | Destination | Protocol | Info                   | Delta      | Lenght |
|-------|-------------|----------------------------|--------------|-------------|----------|------------------------|------------|--------|
| 85180 | 529.518496  | 2010-11-24 18:41:11.576531 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP protocol | 0.000096   | 1514   |
| 85181 | 529.518524  | 2010-11-24 18:41:11.576559 | 10.45.32.180 | 10.45.32.67 | -        |                        | . 0.000038 | 60     |
| 85182 | 529.597908  | 2010-11-24 18:41:11.655943 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.079384   | 1514   |
| 85183 | 529.597956  | 2010-11-24 18:41:11.655991 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000048   | 1514   |
| 85184 | 529.598082  | 2010-11-24 18:41:11.656117 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000126   | 1514   |
| 85185 | 529.598191  | 2010-11-24 18:41:11.656226 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000109   | 1514   |
| 85186 | 529.598330  | 2010-11-24 18:41:11.656365 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000139   | 1514   |
| 85187 | 529.598438  | 2010-11-24 18:41:11.656473 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000108   | 1514   |
| 85188 | 529.598546  | 2010-11-24 18:41:11.656581 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000108   | 1514   |
| 85189 | 529.598824  | 2010-11-24 18:41:11.656859 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000278   | 1514   |
|       | 529.598854  | 2010-11-24 18:41:11.656889 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000030   | 1514   |
| 85191 | 529.598909  | 2010-11-24 18:41:11.656944 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000055   | 1514   |
| 85192 | 529.599048  | 2010-11-24 18:41:11.657083 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000139   | 1514   |
| 85193 | 529.599153  | 2010-11-24 18:41:11.657188 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000105   | 1514   |
| 85194 | 529.599293  | 2010-11-24 18:41:11.657328 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000140   | 1514   |
| 85195 | 529.599392  | 2010-11-24 18:41:11.657427 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000099   | 1514   |
| 85196 | 529.599546  | 2010-11-24 18:41:11.657581 | 10.45.32.180 | 10.45.32.67 | IP       | Fragmented IP rotoco   | 0.000154   | 1514   |
|       | 529, 599578 | 2010-11-24 18:41:11.657613 | 10,45,32,180 | 10.45.32.67 | UDP      | Source port: i d2 De:  | t 0.000032 | 870    |

Fragmented IP packet Very short delta time

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

| 📶 Wireshark: Summ   | iary  |             |     |           |                            |        | × |  |  |  |
|---------------------|---|-------------|-----|-----------|----------------------------|--------|---|--|--|--|
| File                |   |             |     |           |                            |        |   |  |  |  |
| Name:               | E:\sauvegarde\suivi_clients\AEROPORT_NICE\1110\mat_8_2.pcap |             |     |           |                            |        |   |  |  |  |
| Length:             | 126624403 bytes   |             |     |           |                            |        |   |  |  |  |
| Format              | Wireshark/tcpdump/ libpcap                                  |             |     |           |                            |        |   |  |  |  |
| Encapsulation:      |   |             |     |           |                            |        |   |  |  |  |
| Packet size limit:  |   |             |     |           |                            |        |   |  |  |  |
| Time                |   |             |     |           |                            |        |   |  |  |  |
| First packet:       | 2010-11-2   | 24 18:32:22 |     |           |                            |        |   |  |  |  |
| Last packet:        | 2010-11-2   | 24 18:41:18 |     |           |                            |        |   |  |  |  |
| Elapsed: 00:08:56   |   |             |     |           |                            |        |   |  |  |  |
| Capture             |   |             |     |           |                            |        |   |  |  |  |
| Interface:          | unknown   |             |     |           |                            |        |   |  |  |  |
| Dropped packets:    | unknown   | ê.          |     |           |                            |        |   |  |  |  |
| Capture filter:     | unknown   | i.          |     |           |                            |        |   |  |  |  |
| Display             |   |             |     |           |                            |        |   |  |  |  |
| Display filter:     | none  |             |     |           |                            |        |   |  |  |  |
| Traffic             |   | Captured    |     | Displayed | <ul> <li>Marked</li> </ul> |        | • |  |  |  |
| Packets             |   | 86255       |     | 86255     | 0                          |        |   |  |  |  |
| Between first and I | ast packet  | 536,318 sec |     |           |                            |        |   |  |  |  |
| Avg. packets/sec    |   | 160,828     |     |           |                            |        |   |  |  |  |
| Avg. packet size    |   | 1452,024 by | tes |           |                            |        |   |  |  |  |
| Bytes               |   | 125244299   |     |           |                            |        |   |  |  |  |
| Avg. bytes/sec      | _   | 233526,255  |     |           |                            |        |   |  |  |  |
| Avg. MBit/sec       |   | 1,868       |     |           |                            |        |   |  |  |  |
| Hele                |   |             |     |           |                            | Church |   |  |  |  |
| Help                |   |             |     |           |                            | ⊆lose  |   |  |  |  |

Then go in ""Statistics"", ""IO Graph"", and in the new Window enter the following settings : X Axis :

Tick interval : 0,001 sec

Y Axis

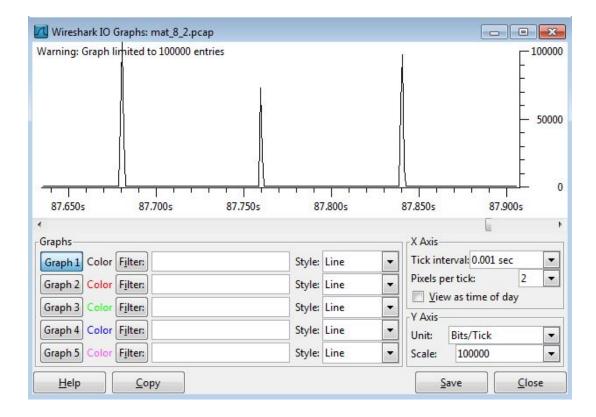
Units : Bits / Tick

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.



×