[Muhammad Zubair Ahmad](https://www.researchgate.net/profile/Muhammad_Ahmad15)[4.33](https://www.researchgate.net/profile/Muhammad_Ahmad15/reputation)

[National University of Science and Technology](https://www.researchgate.net/institution/National_University_of_Science_and_Technology)

**What are the best opensource tools for packet capturing in network research. The aim is minimize packet losses experienced in wireshark(50%)?**

Different solutions have been employed but packet loss ratio is very high. The best up till now has been wire-shark. Kindly guide as to how we can increase the capture ratio and what software are commonly used in the community for this purpose.

Thanks in advance for your help.

**TOPICS**

* [WiFi](https://www.researchgate.net/topic/wifi?ev=tp_pst_dtl_xkey)
* [Network Administration](https://www.researchgate.net/topic/network_administration?ev=tp_pst_dtl_xkey)
* [Network Architecture](https://www.researchgate.net/topic/network_architecture?ev=tp_pst_dtl_xkey)
* [Network Analysis](https://www.researchgate.net/topic/network_analysis?ev=tp_pst_dtl_xkey)
* [Network Traffic Simulation](https://www.researchgate.net/topic/network_traffic_simulation2?ev=tp_pst_dtl_xkey)
* [Internet Applications](https://www.researchgate.net/topic/internet_applications?ev=tp_pst_dtl_xkey)
* [Wireshark](https://www.researchgate.net/topic/wireshark?ev=tp_pst_dtl_xkey)
* [](https://www.researchgate.net/profile/Andrea_Piroddi)

[**Andrea Piroddi**](https://www.researchgate.net/profile/Andrea_Piroddi) · Netconsulting2008, Rome, Italy

you can find interesting OpenNMS ([http://www.opennms.org/](https://www.researchgate.net/go.Deref.html?url=http%3A%2F%2Fwww.opennms.org%2F)) and Capsa Free ([http://www.colasoft.com/capsa-free/](https://www.researchgate.net/go.Deref.html?url=http%3A%2F%2Fwww.colasoft.com%2Fcapsa-free%2F)). Another one is a web based network tool Xymon  that you can find at[http://sourceforge.net/projects/xymon/](https://www.researchgate.net/go.Deref.html?url=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fxymon%2F). In my opinion OpenNMS is what you're searching for.

 9 days ago

* [](https://www.researchgate.net/profile/Matthias_Wilhelm2)

[**Matthias Wilhelm**](https://www.researchgate.net/profile/Matthias_Wilhelm2) · [35.73](https://www.researchgate.net/profile/Matthias_Wilhelm2/reputation) · [14.14](https://www.researchgate.net/profile/Matthias_Wilhelm2/publications) · Toyota InfoTechnology Center, Tokyo, Japan

Can you give more details on what you are looking for? It sounds like your Wireshark causes packet loss during capture, but I don't think that is likely. The software just puts a network interface in listening mode and receives all packets, even packets that are not addressed to your machine. It is not a computationally expensive task, so I can't think of a reason Wireshark should cause losses. At least other software will have the same problem, they probably also use the standard libpcap to capture the packets.

[2](javascript:) / 0 · 9 days ago

* [](https://www.researchgate.net/profile/Ankit_Mundra)

[**Ankit Mundra**](https://www.researchgate.net/profile/Ankit_Mundra) · [2.38](https://www.researchgate.net/profile/Ankit_Mundra/reputation) · [0](https://www.researchgate.net/profile/Ankit_Mundra/publications) · [The Central University of Rajasthan](https://www.researchgate.net/institution/The_Central_University_of_Rajasthan)

cisco packet tracer or OpenMP

[1](javascript:) / 0 · 9 days ago

* [](https://www.researchgate.net/profile/Shihab_Hameed4)

[**Shihab A. Hameed**](https://www.researchgate.net/profile/Shihab_Hameed4) · [11.41](https://www.researchgate.net/profile/Shihab_Hameed4/reputation) · [0.7](https://www.researchgate.net/profile/Shihab_Hameed4/publications) · [International Islamic University Malaysia](https://www.researchgate.net/institution/International_Islamic_University_Malaysia)

you can try this Portable network analyzer(packet sniffer) freeware.

[http://www.colasoft.com/capsa-free/](https://www.researchgate.net/go.Deref.html?url=http%3A%2F%2Fwww.colasoft.com%2Fcapsa-free%2F)

[1](javascript:) / 0 · 9 days ago

* [](https://www.researchgate.net/profile/Luis_Sequeira2)

[**Luis Sequeira**](https://www.researchgate.net/profile/Luis_Sequeira2) · [5.99](https://www.researchgate.net/profile/Luis_Sequeira2/reputation) · [2.29](https://www.researchgate.net/profile/Luis_Sequeira2/publications) · [University of Zaragoza](https://www.researchgate.net/institution/University_of_Zaragoza)

I always use tcpdump and prefer to develop my own scripts for processing the traces.

[1](javascript:) / 0 · 7 days ago

* [](https://www.researchgate.net/profile/Taner_Karagol)

[**Taner Karagol**](https://www.researchgate.net/profile/Taner_Karagol) · [ASELSAN Inc.](https://www.researchgate.net/institution/ASELSAN_Inc)

Explain your setup please. Are you capturing local computer on which wireshark also running. Or you are capturing by using mirroring port. Loss can be any place. Anyway, I will recommend tcpdump. Dont use graphical tools, graphics always increase CPU load and so increase possibility of packet loss.

 6 days ago

* [](https://www.researchgate.net/profile/Luis_Sequeira2)

[**Luis Sequeira**](https://www.researchgate.net/profile/Luis_Sequeira2) · [5.99](https://www.researchgate.net/profile/Luis_Sequeira2/reputation) · [2.29](https://www.researchgate.net/profile/Luis_Sequeira2/publications) · [University of Zaragoza](https://www.researchgate.net/institution/University_of_Zaragoza)

 I agree with Taner Karagol, the capture environment is an important point. A sniffer which does not degrade the performance of the applications/network traffic has to be included at the best location for capturing.

 6 days ago

* [](https://www.researchgate.net/profile/Yousef_Darmani)

[**Yousef Darmani**](https://www.researchgate.net/profile/Yousef_Darmani) · [1.26](https://www.researchgate.net/profile/Yousef_Darmani/reputation) · [0.65](https://www.researchgate.net/profile/Yousef_Darmani/publications) · [Khaje Nasir Toosi University of Technology](https://www.researchgate.net/institution/Khaje_Nasir_Toosi_University_of_Technology)

I used wire shark in many test environments without any lost packets at all. Are you sure that all your packets are getting to your computer? I am in doubt about your hub. Actually, if you use a switch or a hub able to learn MAC addresses, you will experience the same problem. Use a very simple and old HUB instead.

 4 days ago

* [https://c5.rgstatic.net/m/1951093203564/images/template/default/profile/profile_default_s.jpg](https://www.researchgate.net/profile/Sergio_Alves8)

[**Sergio Alves**](https://www.researchgate.net/profile/Sergio_Alves8) · [Institute of Telecommunications](https://www.researchgate.net/institution/Institute_of_Telecommunications)

Packet losses can happen due to your physical medium channel (copper cable, radio link, optical fiber), network equipments malfunction/configuration, network topology or QOS, or be related with one or both of your network endpoints (which includes network stack, protocols, etc). And these packets are really losses, which means that the packet information get lost at some point and the receiver never receives it.

But you may be experiencing another type of "packet loss" which can be caused by wireshark (or other capturing tool) itself and it is usually called "dropped packets". This type of loss is shown in the wireshark status bar, alongside with the number of packets captured, displayed and marked statistics. PLEASE NOTE that this information is only displayed if Wireshark was unable to capture all packets [refer to[https://www.wireshark.org/docs/wsug\_html\_chunked/ChUseStatusbarSection.html](https://www.researchgate.net/go.Deref.html?url=https%3A%2F%2Fwww.wireshark.org%2Fdocs%2Fwsug_html_chunked%2FChUseStatusbarSection.html) ], which allows you to immediately infer if this is your situation. Please note also that this metric IS NOT SAVED in your pcapng files; you can see it - if it occurs - while capturing or even after you stop the capture process but still displaying the capture in the wireshark; even if you save that capture, once you close it, you will not see this metric again.

This type of packet loss relates with the performance of the capturing system, usually due to your hard drive read/write rate and overall system load. What happens in this situation is that wireshark was able to detect one or more packets in the capture network interface, but due to the low performance, it could not save the related packet information, so the capture algorithm chooses to drop that packet(s). There are some tricks you can follow to minimize (not avoid!) the low performance impact, which are explained in the "optimized Wireshark settings" section,[https://wiki.wireshark.org/Performance](https://www.researchgate.net/go.Deref.html?url=https%3A%2F%2Fwiki.wireshark.org%2FPerformance" \t "_blank) . Note also, that the operating system has an important role in the performance; some time ago, while facing some problems related to this, I discover that the number of packets dropped by wireshark on Linux was (much!) less while capturing with Wireshark on Windows - what was not really a surprise for me. Notice that the performance issue can also happen with other software tools. I will assume that you are not generating network traffic in the same capture system, because this negatively influences the performance too.

If you are dealing with optical fiber links, I advise you to - if possible - forget wireshark or similar software tools and use instead a dedicated network performance measure equipment. These kind of equipments usually have dedicated high performance hardware, like FPGAs, that will allow you to generate all kind of network traffic and get almost all measures and statistics you may desire or need.

From my personal experience, considering a I7 Quad Processor, with 16GB RAM but a mechanical 5400rpm or 7200rpm HDD, when considering a large number of packets, from time to time - say 1 in 10/15 times - I was facing dropped packets even on a 1Gbps ethernet link. The problem was more notorious as the number of packets increases (typically for < 1 million packets it were dropped less than 1k packets but for 9 M, the number of dropped packets increases to 3M easily!). Although I successfully reduced the number of packets dropped, I could not avoid the problem because from time to time, I still get some dropped packets, which do not allow me to have 100% confidence in my measures.

Since at the beginning I have no access to a dedicated Network Performance measure hardware, I developed a simple measure system based on FPGA that allow me to despite this problem and prove the correct system function.

I hope that this information can help you.



**Fred Kashefi** · [University of Texas at Arlington](https://www.researchgate.net/institution/University_of_Texas_at_Arlington)