

Differences between Real-Time Traffic Analysis and Packet Analysis in AthTek NetWalk

AthTek NetWalk supports both real-time and postmortem analysis. Do you know what the differences are? Most of time, real-time and postmortem analysis shares the same template to analyze the traffic data. Real-time traffic analysis shows dynamic trends of the entire network, while postmortem traffic analysis shows exactly what has happened in this network. In this article, you will read the main differences between real-time traffic analysis and packet analysis in [AthTek NetWalk](#).

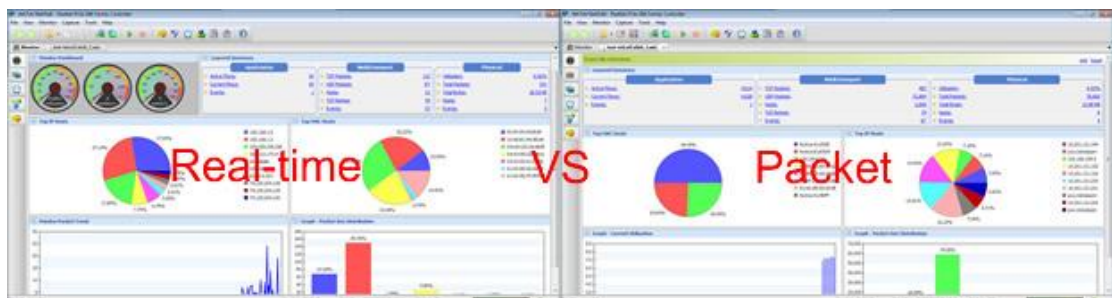


VS



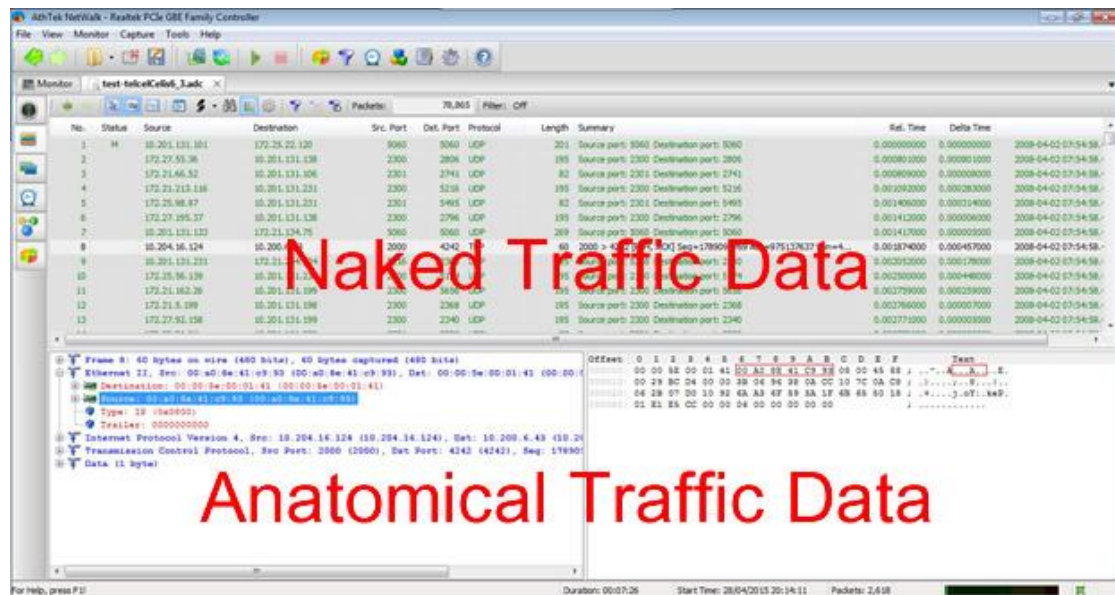
1. Overview.

In Overview section, real-time traffic shows current bandwidth usage and accumulated traffic data. But if you opened a captured packet in AthTek NetWalk, you will see fixed values of the network traffic and these values tell you exactly what has happened during the capturing period.



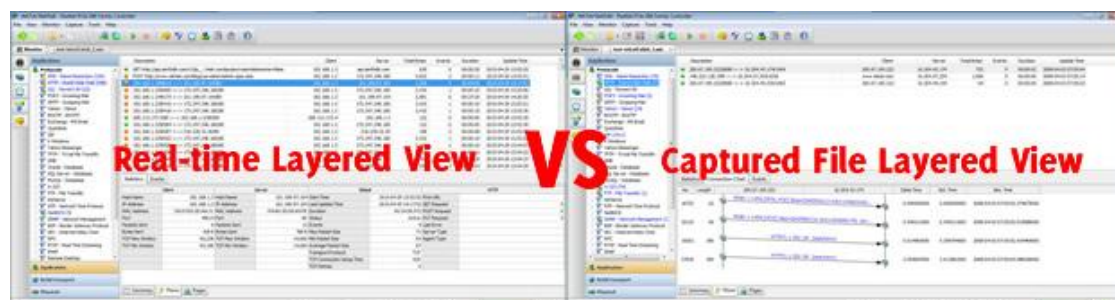
2. Packets.

When you opened a captured file in AthTek NetWalk, you will see a new tab named "Packets" created on left. Real-time traffic analysis doesn't support Packets tab. In Packets tab, network administrators can read all the communication details including requested IP addresses, ports, protocol, etc. If a common packet analyzer enables network administrator to see a naked data, AthTek NetWalk enables users to see a reliable anatomical traffic data through detail and hex view tool.



3. Layered View.

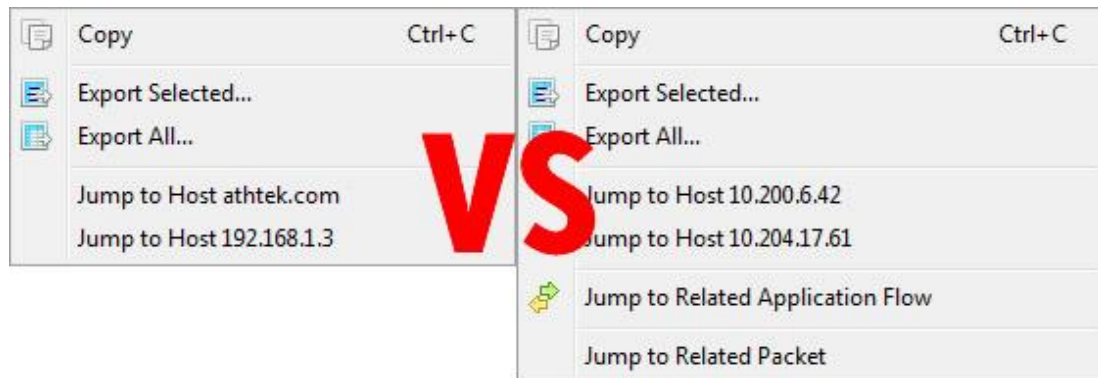
There are 3 layers in Layered View section: Application, Net&Transport and Physical. A significant different is, you can see communication flows in postmortem packet analysis.



4. Events Tab.

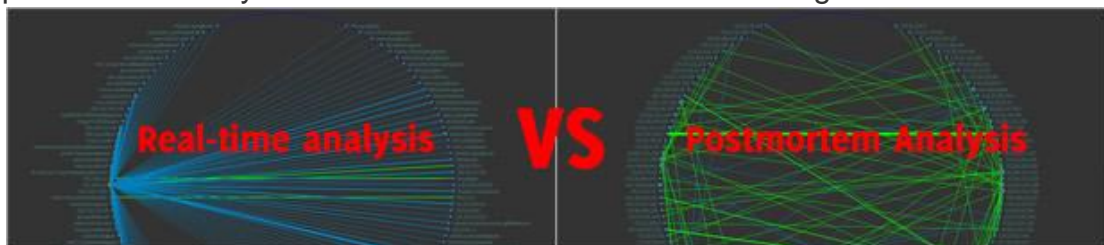
In Events tab, network administrator can jump to the communication flow when

it is a postmortem packet analysis.



5. Matrix Map.

In Matrix Map, real-time analysis only marks active connections in green, while postmortem analysis marks all successful connections in green.



In short, postmortem analysis enables network administrators to see all communication details happened on the network. All you need to do is to capture packets and open the captured file in AthTek NetWalk.