VIT Vidyalankar Institute of Technology
Accredited A+ by NAAC

DEPARTMENT OF COMPUTER ENGINEERING
Computer Network Lab

Semester	T.E. Semester V – Computer Engineering
Subject	Computer Network
Subject Professor In-charge	Prof. Amit K. Nerurkar
Assisting Teachers	Prof. Amit Alyani
Laboratory	313-A

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Study Of Traffic Analysis tool's

1.WireShark

2.Liveactionomnipeek

3.etherape

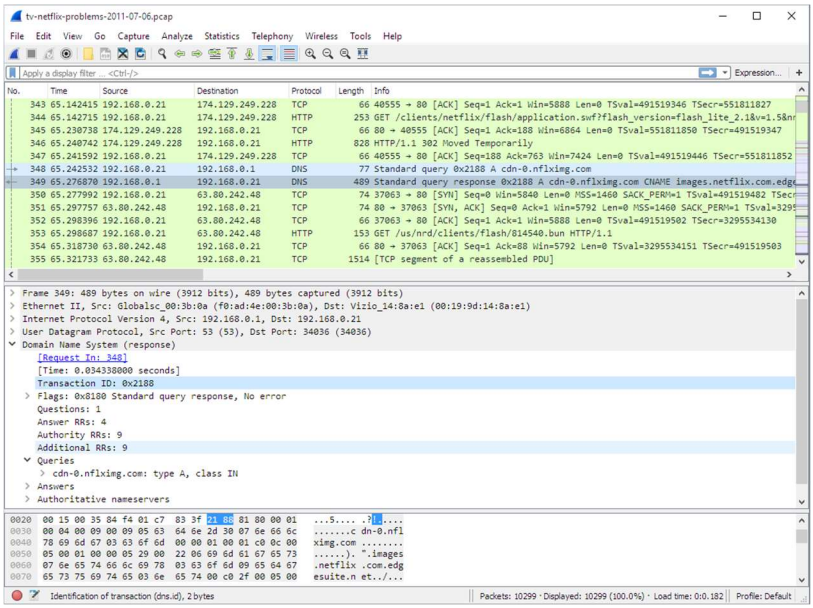
1.WireShark

1.1. What is Wireshark?

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with



the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

2.LiveAction OmniPeek

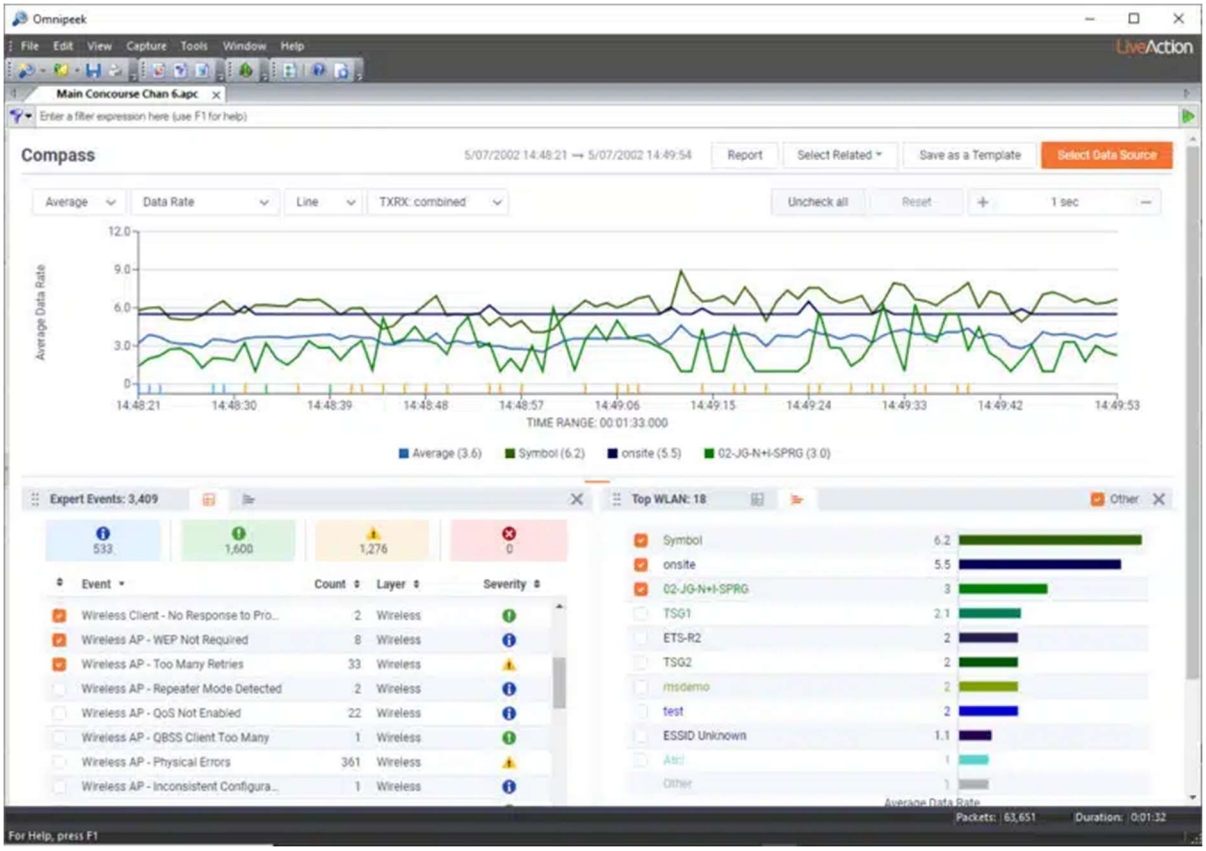
LiveAction OmniPeek is a sophisticated network analysis and monitoring tool used for in-depth examination of network traffic and performance. It allows network administrators and IT professionals to gain a comprehensive understanding of their network infrastructure through the following key features:

1. **Packet Capture and Analysis:** OmniPeek can capture data packets as they traverse the network. This includes Ethernet, Wi-Fi, and other protocols. It then provides a detailed breakdown of each packet, allowing users to inspect the contents, headers, and metadata.
2. **Real-Time Monitoring:** It offers real-time monitoring capabilities, providing live statistics on network utilization, bandwidth consumption, and other performance metrics. This helps in promptly identifying and addressing network bottlenecks and anomalies.
3. **Protocol Analysis:** OmniPeek supports a wide range of network protocols, including TCP/IP, HTTP, FTP, DNS, and more. Users can analyze the behavior of these protocols to pinpoint issues or security threats.
4. **Network Visualization:** The tool often provides visual representations of network traffic flows and patterns, making it easier to understand complex networks and spot irregularities.
5. **Traffic Filtering and Search:** Users can apply filters to isolate specific types of traffic or criteria, which is particularly useful for investigating issues or monitoring specific network activities.
6. **Expert Analysis:** OmniPeek includes expert analysis tools that automatically detect and flag potential network problems or security risks. It can also provide recommendations for remediation.

7. **Historical Analysis:** Beyond real-time monitoring, the tool allows users to review historical data, making it possible to trace network issues back in time to identify trends or recurring problems.

8. **Remote Packet Capture:** OmniPeek can capture network packets remotely from various locations, which is beneficial for analyzing distributed networks or troubleshooting issues in different parts of an organization.

9. **Reporting:** It offers reporting capabilities to document network performance and issues for further analysis or compliance purposes.



Overall, LiveAction OmniPeek is a robust network analysis tool that provides deep insights into network behavior and helps organizations maintain, optimize, and secure their networks effectively. It is a valuable asset for those responsible for managing and ensuring the reliability of complex computer networks.

3. Etherape

EtherApe is a graphical network monitoring tool used to visualize network traffic activity in real-time. Here are some key details about EtherApe:

1. **Real-Time Network Visualization:** EtherApe displays a dynamic and animated graph that represents network traffic flows between different hosts on a network. Each host is represented by a node, and the connections between them are depicted as lines. The size and color of nodes and lines correspond to the volume and type of traffic, allowing users to quickly identify the most active hosts and communication patterns.

2. **Protocols and Traffic Types:** EtherApe provides information about the types of traffic being transmitted on the network, such as TCP, UDP, ICMP, and more. It can also differentiate between various protocols and services, making it useful for identifying the sources and destinations of network traffic.

3. **Ease of Use:** This tool is designed with a user-friendly interface that makes it accessible to both novice and experienced users. The graphical representation simplifies the process of understanding network activity, making it easier to spot potential issues or anomalies.

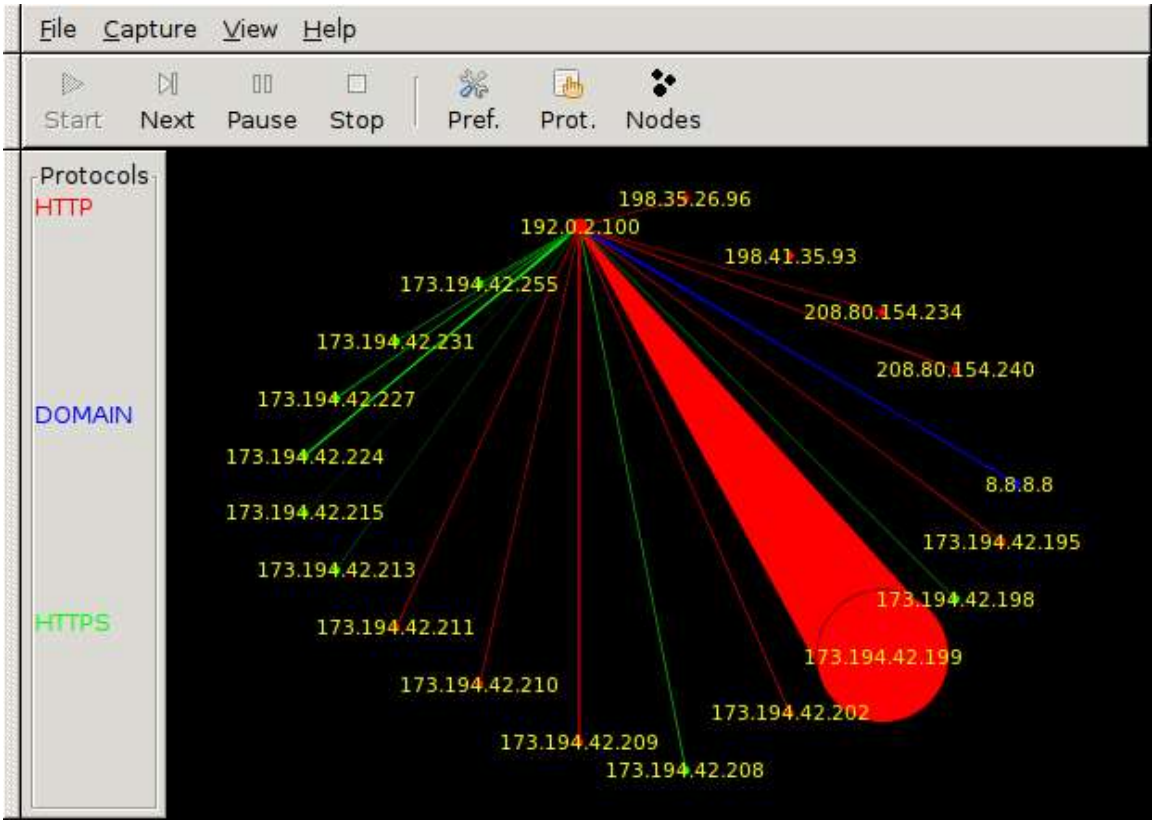
4. **Packet Capture:** While EtherApe primarily focuses on real-time network visualization, it also has the capability to capture network packets for more in-depth analysis when needed. Users can export captured packets for further examination using other tools.

5. **Cross-Platform Compatibility:** EtherApe is available for various operating systems, including Linux, Unix, and macOS. This cross-platform support makes it versatile and widely accessible.

6. **Open Source:** EtherApe is an open-source tool, which means it is freely available for anyone to use and modify. This fosters a community of developers who can contribute to its ongoing development and improvement.

7. **Network Troubleshooting:** Network administrators and IT professionals often use EtherApe for troubleshooting network performance issues, identifying

bandwidth hogs, and assessing network health. It can help pinpoint the source of congestion or unusual network behavior.



In summary, EtherApe is a real-time network monitoring and visualization tool that provides a visual representation of network traffic patterns. It is particularly valuable for network administrators and analysts who want to quickly understand the state of their networks, identify potential problems, and optimize network performance. Its user-friendly interface and open-source nature make it a popular choice among network professionals.