
TraceRoute Tool

Introduction and Features

The Kane Security Analyst main menu bar consists of six options. The **TraceRoute Tool** is located under the **Add-Ins** option within the **Network Tools** group.

The reason for integrating this tool with Kane Security Analyst is to allow Security Administrators to perform reachability/network-debugging activities from within the Analyst console. The GUI-based **TraceRoute Tool** that ships with Kane Security Analyst 5.1 contains many improvements over the console-based TraceRoute tool that ships with Windows NT.

Major features of the Analyst **TraceRoute Tool** include:

- The tool has a full-fledged GUI that helps you effectively use the tool.
- The **TraceRoute Tool** ships with flexible customization options. The options include time between packets sent, packet timeout values, and maximum number of hops (from the source to the destination machine).
- Comprehensive statistics. After completion of a TraceRoute activity, the tool generates comprehensive statistics that include number of packets sent, number of packets received, percent loss, and so on.
- This tool is tightly integrated with Kane Security Analyst; that is, the tool can be invoked only through Kane Security Analyst and it cannot be invoked separately.
- In the evaluation version, the **TraceRoute Tool** expires along with Kane Security Analyst.

Startup

Use the following steps to run the **TraceRoute Tool**:

- Step 1** Start the **TraceRoute Tool** by selecting **Add-Ins** on the Analyst main menu.
- Step 2** Click **Network Tools>TraceRoute**. The **TraceRoute** window shown in Figure 1 displays.

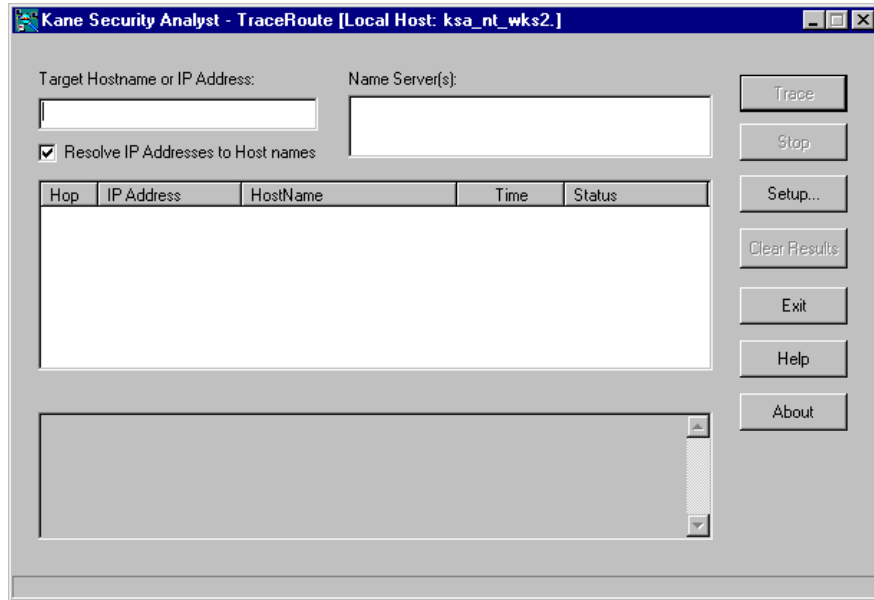


Figure 1 Network Tools TraceRoute Window

- Step 3** Type in a target host name (for example, www.xyzzzy.com) or IP address in the format a.b.c.d. The tool displays the list of name servers which it will use to resolve the host name into a valid IP address. The list of name servers discovered by the tool is limited to a maximum of two: primary and secondary DNS servers. After you type in a name or IP address, the **Trace** button is activated.
- Step 4** You can have an IP address resolved automatically (by doing a DNS lookup) and displayed as a name by clicking on the checkbox for **Resolve IP Addresses to Host Names**. The result will be displayed in the **Statistics** box upon the completion of operation.
- Step 5** Click the **Setup** button to display the KSA **TraceRoute Setup** window, as shown in Figure 2. The setup window gives you several packet transmission options. The **TraceRoute Setup** window allows you to select the packet timeout limit, as well as packet data length to look for, and the maximum number of hops.

Maximum number of Hops: This represents the maximum value for hops (1 – 255)

Packet Timeout (milliseconds): Timeout between packet sent and packet received (1 – 30000 ms)

Packet Data Length (in bytes): The data portion of the packet (8 – 16384 bytes).

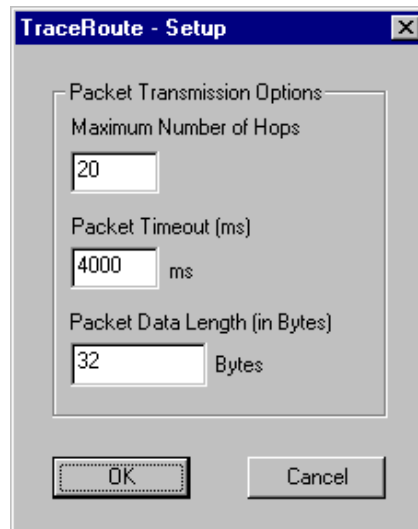


Figure 2 Network Tools TraceRoute Setup Window

Step 6 Click **Trace** to start. Click **Stop** to stop.

Step 7 Click **Clear Results** to start again.

Step 8 Click **Exit** to stop the program and exit.

Viewing the Results

Once a **TraceRoute Tool** operation is complete or you stop the tool, the tool displays the necessary overall statistics. This includes number of packets sent, number of packets received, percent loss (number sent – number received)/ number sent * 100), and the average round trip times.

Display of the Results

The output of the TraceRoute operation is displayed in the results window.

- **Hop:** Hop Count. The number of hops from the source to the destination machine.
- **IP Address:** IP address on the received packet
- **Host name:** Host name for that IP address (performed by a reverse DNS look up)
- **Time:** The round trip time (computed based on the time stamp differences between sent and received packet)
- **Status:** The status of the operation.
- **TTL Expired:** Intermediate Gateway/Router
- ***:** Unable to trace a route
- **Host Reached:** Host is reached
- **Statistics Window:** Outputs the statistics of a TraceRoute operation.