

Unispeed Netlogger FT 3.0 Release notes

Unispeed A/S
Engvej 139,
DK2300 København S
33445500, fax 33445501
www.unispeed.com



The netlogger FT 3.0 release is the most comprehensive software update ever issued by Unispeed. The update includes a complete redesign of the K-sniffer, zero copy subsystem, the design and functionalities of the Netlogger workbench now called the Netlogger Frontend and redesign of several of the tools plus introducing a few new ones.

.....

Table of Contents

Hardware accelerated K-sniffer.....	2
FT 3.0	2
Tools.....	2
Examples.....	3

Hardware accelerated K-sniffer

The Unispeed K-sniffer has undergone several improvements compared to the 2.4 version, and now fully supports and utilises multi-core processors from both AMD and Intel, Pci express and up to 8 x 1Gbit network interfaces at full line speed.

10 Gbps Network-cards are currently being integrated in the Netlogger system, and will be available during this summer.

FT 3.0

The FT 3.0 framework has undergone several modifications and modernisations.

The design has changed to a more modern and user friendly lay-out with extensive use of drop down menus and multiple canvas areas.

The overall stability and data security has been greatly improved to avoid packet loss and system breakdowns.

Mitigation and integration with third party databases has been improved and is easily available and can be configured in seconds via the tool menu.

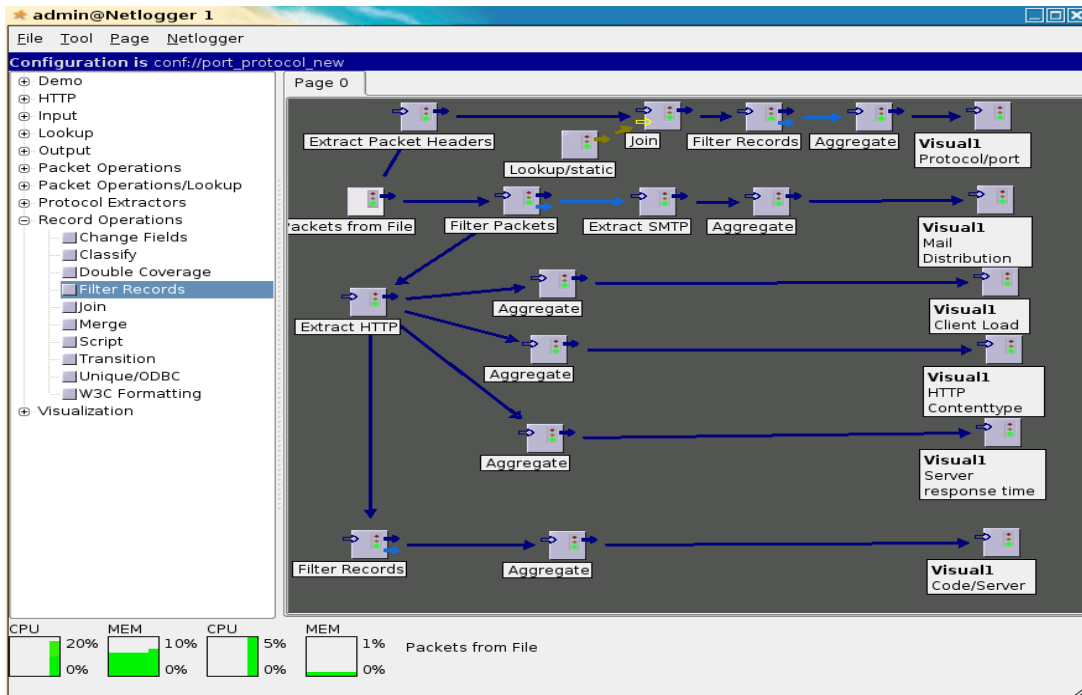
Tools

All Tools now have a drop down allowing the user to start and stop the tool, configure and annotate the tool and see the output from each individual tool.

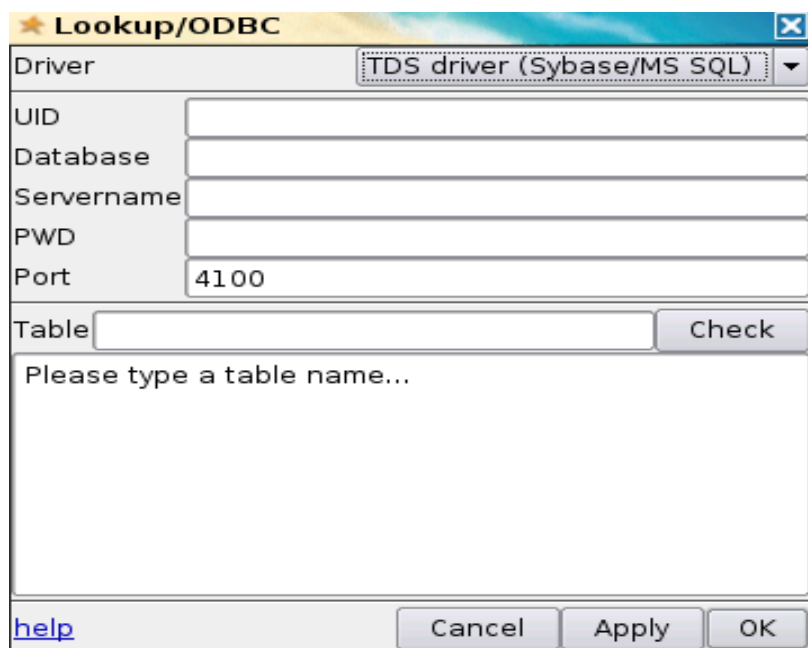
Several new tools has been added to the Netlogger including

- Forward packets: enables the Netlogger to forward packet-streams to other Netloggers or third party tools, thus increasing the scalability and the usability of the Netlogger system.
- Session info: tool which extract sender and receiver IP address and port-numbers, transport protocol and time stamp for start and end of a session.(the tool is mainly for European anti-terror legislation requirements)
- Session logging: tool that logs data from session info to binary files
- Protocol detect: tool which detects certain protocols irrespectively from the port number it was send to/from
- Visualisation: tool which can visualise the output from one or more aggregate tools, and give the user a quick overview about the traffic composition, server response times, server response codes or other traffic information that is best analysed in a graphical manner.
- And a few more protocol extractors

Examples



Canvas area with tools annotated



The 'Lookup/ODBC' dialog box is shown with the following fields and controls:

- Driver:** TDS driver (Sybase/MS SQL) (dropdown menu)
- UID:** (empty text field)
- Database:** (empty text field)
- Servename:** (empty text field)
- PWD:** (empty text field)
- Port:** 4100 (text field)
- Table:** (empty text field) with a **Check** button to its right.
- Message:** Please type a table name... (text area)
- Buttons:** help (link), Cancel, Apply, and OK.

Configuring a tool

The screenshot shows the unispeed configuration interface. The main workspace displays a workflow diagram with components like 'Packets from Network', 'Session Info', 'Change Fields', 'Join', 'Log to Database/ODBC', 'Log to File', 'LookUp/ODBC', 'Traffic Measurement', 'Bandwidth Measurement', and 'Script'. On the right, several data windows are open, showing sample outputs for 'Packets from Network samples...', 'Session Info samples...', 'Change Fields samples...', and 'LookUp/ODBC' settings.

Output shown for several tools

This screenshot displays a more complex workflow diagram with components such as 'Packets from File', 'Filter Packets', 'Extract SMTP', 'Aggregate', 'Visual1', 'Extract HTTP', 'Aggregate', 'Visual1', 'Aggregate', 'Visual1', 'Filter Records', 'Aggregate', 'Visual1', 'Extract Packet Headers', 'Aggregate', and 'Visual1'. Below the workflow, several tool outputs are shown as horizontal bar charts:

- server load**: A chart showing server IP keys and their corresponding length sums.
- Tool 12**: A chart showing server IP keys and their average response times.
- Tool 8**: A table showing content types and their lengths.
- Tool 19**: A chart showing sender keys and their largest mail sizes.
- Tool 15**: A chart showing server IP keys and their counts for codes greater than 200.

Real-time visualisation