

# The MOME Meta-Database for Monitoring and Measurement Tools and Traces

**MOME**

Felix Strohmeier, Salzburg Research

**21st TF-NGN Meeting**

4-5 July 2006

Ljubljana, Slovenia



# Outline

- | Short Intro – the MOME project
- | The MOME Database
  - | Meta-Data Approach
  - | MOME Trace Database
  - | MOME Tools Database
- | Automatic Analyses
- | Current Setup
- | Interfaces
  - | GUI, PUT/GET
- | Current Data
- | Outlook

## Short Intro – the MOME project



- | FP6 IST project, EU Strategic Objective „Broadband for all“
  - | “Co-ordination Action” January 2004 – March 2006
- | Overall Objective

**Co-ordinate activities  
in the field of IP monitoring and measurement**

- | Promote co-operation between IST projects

**Measurement Tools**

**Measurement Data**

**Measurement  
Standardisation**

- | Exchange knowledge via

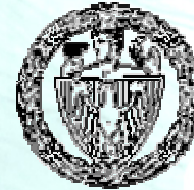
**Workshops, Conference Sessions, Webpage**



# MOME Consortium

MOME

salzburg|research



Salzburg Research, AT

NEC, UK

Telefónica I+D, ES

Université Libre de Bruxelles, BE

Budapest University of Technology  
and Economics, HU

Politechnika Warsaw, PL

Fraunhofer FOKUS, DE

TERENA, NL



NEC

*Telefonica*



**Total: 65 PM**

# The Need for Measurement Data and Tools

- | Developing new measurement and monitoring methods
- | Developing architectures of measurement and monitoring systems
- | Developing algorithms for network and traffic control functions supported by measurements
- | Developing and validating realistic traffic models
- | Validating the SLA-specified QoS

Easy access to the repositories of raw measurement data is highly desirable

Easy access to information about available measurement tools is highly desirable

The ultimate goal: „Understanding the Internet“

# The MOME Database

MOME

- | The Meta-Data Approach
- | MOME Tools Database
- | MOME Trace Database

# The Meta-Data Approach

- | Projects generate public available measurement data
  - | Intrusion detection evaluation sets
  - | Traffic traces of different applications
  - | Traffic matrices
  - | BGP traces
  - | IPv6 measurement traces
  - | Wireless traffic traces
  - | ...
- | Hard to find by search engines
- | Provide a central place for access
- | Include more information than just links
  - | Make entries comparable and searchable

# The Meta-Data Approach

- | „Data about data“
  - | Documentation of measurement environment and scenario
  - | Statistical information about the captured traffic
  - | Link to the repository, where data is actually stored
  
- | „Data about tools“
  - | Categorisation
  - | Measured metrics
  - | Hardware and software platform

MOME assists researchers in finding and retrieving the measurement data and tools that are most appropriate for their purposes

# The Meta-Data Approach

MOME

- | Distributed storage of measurement data
  - | As much storage as provided by the sources of the measurements
- | Centralised 'directory' functionality to access the measurement data
  - | Directory stores data about the remotely stored measurement data
  - | Amount of data is minimal compared to the raw data
- | Projects contributing measurements can keep total control on them
  - | When they withdraw data from public access
    - | They delete the entry in the MOME database
    - | The MOME database itself detects when registered measurements have been withdrawn from the Internet
- | Other Examples
  - | CAIDA's IMDC (public service just started)
  - | GRID technology based solar observatory

# MOME Tools Database



- | Similar to Freshmeat and others
- | Specialised for Monitoring and Measurement Tools
- | Tools Categories
  - | Packet Capturing
  - | Traffic Flow Measurement
  - | Packet Monitoring
  - | Connection Monitoring
  - | Application Level Monitoring
  - | Service Monitoring
  - | Accounting
  - | Intrusion Detection
  - | Sniffing
  - | Performance Monitoring
  - | Connectivity Checking
  - | Route Detection
  - | Topology Detection
  - | Traffic Visualization
  - | Traffic Generation
  - | Bandwidth Measurement

# MOME Tools Database



## | Stored Meta-Information

- | Availability
- | Maturity
- | Version Info
- | License Information
- | Measured Metrics
- | Supported Protocols
- | Supported Platforms
- | Measurement Methods
- | Measurement Algorithms
- | Interfaces
  - | Control
  - | Data
- | Interoperability with other Tools

## | Further Information

- | Tool Maintainer
- | User Comments

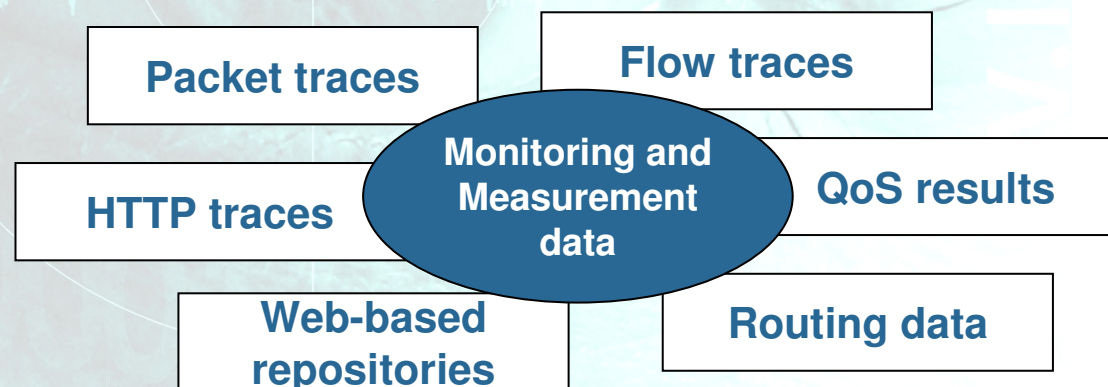
## | Links

- | Homepage
- | Contact
- | Related URLs

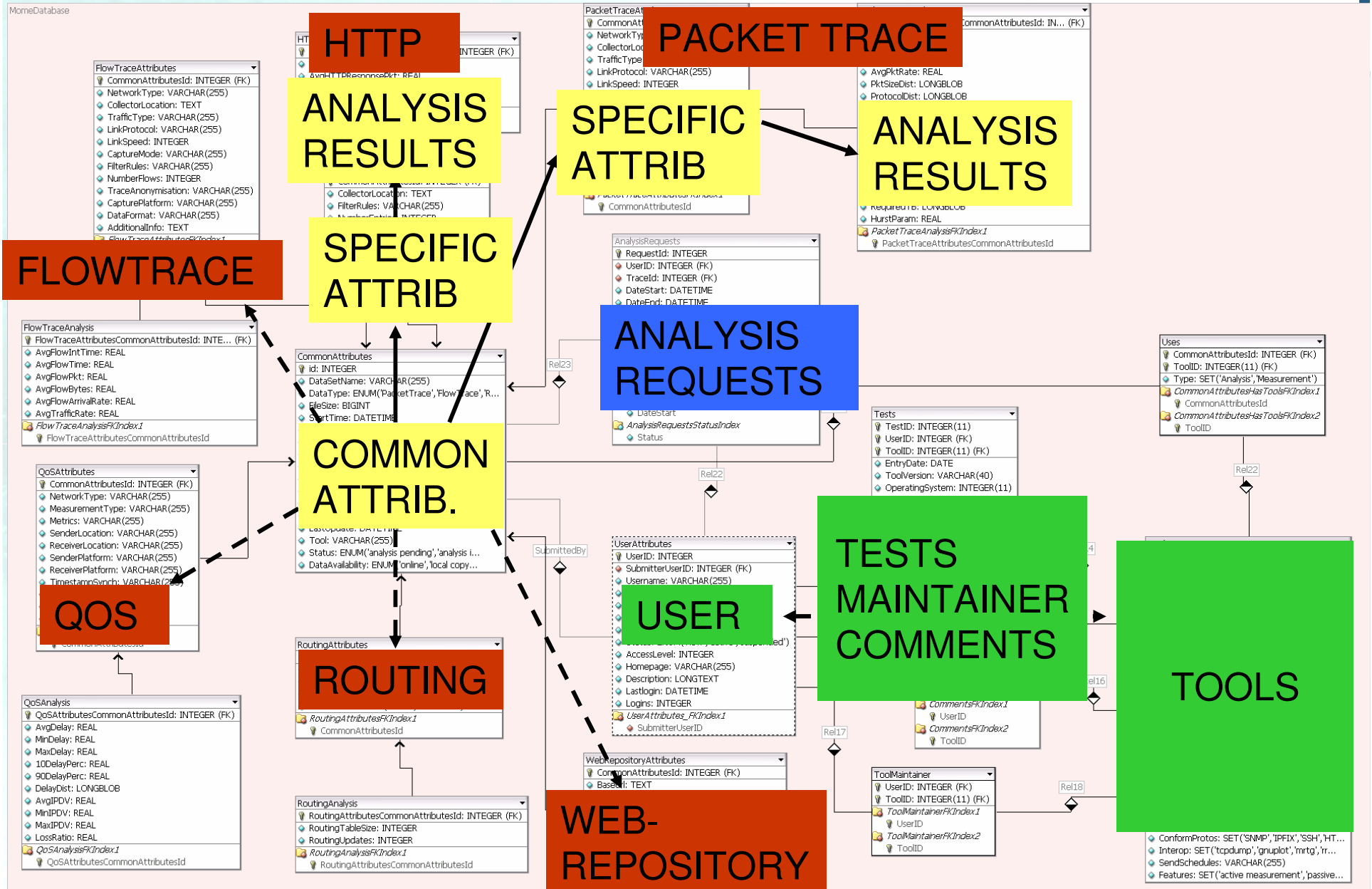


# MOME Trace Database

- | A database model suited for heterogeneous measurements
  - | Different kinds of measurements
  - | Measurements produced by different tools
- | Meta-data model
  - | Describe the actual data of interest
- | Trade-off: keep it generic – keep it specific



# MOME Database Model - Overview



# MOME Database Model

## Packet traces

Dataset name	FH-SBG 2005-01-28@18:00
Data type	PacketTrace
File size	15.6MB
File compression	bz2
Start time	2005-01-28 18:00:00
End time	2005-01-28 18:59:00
Duration	0:59:00
Description	Trace FH Salzburg
Dataset location	URL: <a href="http://shell.ist-mome.org/traces/PacketTrace/2005-01-28@18:00.pcap.bz2">http://shell.ist-mome.org/traces/PacketTrace/2005-01-28@18:00.pcap.bz2</a>
MD5 Sum	a12627bcb53164aa22e3e742014886ed
Tool	tcpdpriv
Submitted by	fh-sbg @ 2005-01-29 00:18:00
Last Update	2005-02-02 17:30:08
Availability	local copy



Raw data

Network Type	WAN Access Network
Collector Location	AT, Salzburg, FH Salzburg
Traffic Type	Operational Traffic, Educational Institution
Link Protocol	X.21
Link Speed	4.0Mbps
Capture Mode	mirror port
Filter Rules	none
Trace Anonymisation	-P99 -A50
Capture Platform	Linux 2.6.9
Data Format	libpcap
Additional Info	2x2Mbps X.21 connections

# MOME Database Model

## Flow traces

<b>Dataset name</b>	Abilene NetFlow stats report, router Atlanta, 31.12.2004
<b>Data type</b>	FlowTrace
<b>File compression</b>	none
<b>Start time</b>	2004-12-31 00:00:00
<b>End time</b>	2004-12-31 23:59:59
<b>Duration</b>	23:59:59
<b>Description</b>	Daily summaries of NetFlow reports from the Internet2 Abilene backbone network.
<b>Dataset location</b>	URL: <a href="http://www.itec.oar.net/cgi-bin/abi...-Detail&amp;format=HTML&amp;sort=-&amp;lines=25">http://www.itec.oar.net/cgi-bin/abi...-Detail&amp;format=HTML&amp;sort=-&amp;lines=25</a>
<b>Tool</b>	NetFlow
<b>Submitted by</b>	mdabrowski @ 2005-02-04 11:01:33
<b>Last Update</b>	2005-02-04 11:01:33
<b>Availability</b>	unavailable

<b>Network Type</b>	WAN
<b>Collector Location</b>	Atlanta, US
<b>Traffic Type</b>	operational traffic, WAN
<b>Link Protocol</b>	n/a
<b>Capture Mode</b>	from router, NetFlow
<b>Filter Rules</b>	none
<b>Trace Anonymisation</b>	none
<b>Capture Platform</b>	n/a
<b>Data Format</b>	text file
<b>Additional Info</b>	The raw NetFlow data sets are available only on request. Public access is offered to daily and weekly summaries. Reports are created by the ♦ flow-tools ♦ software and can be viewed in the form of HTML table or plain ASCII format.



Raw data

# MOME Database Model



QoS measurements

Dataset name	NLANR AMP QoS measurement, 03.02.2005
Data type	QoS
Start time	2005-02-03 00:00:00
End time	2005-02-03 23:59:59
Duration	23:59:59
Description	One-day QoS measurements performed by the Active Measurement Project (AMP) architecture, between nodes amp_aarn, to amp_asu/105.2.3, measuring round trip time (RTT), packet loss, topology, and throughput.
Dataset location	URL: <a href="http://watt.nlanr.net/active/cgi-bin/daily/asu/105.2.3">http://watt.nlanr.net/active/cgi-bin/daily/asu/105.2.3</a>
Tool	IPMP
Submitted by	mdabrowski @ 2005-02-04 10:24:44
Last Update	2005-02-04 10:24:44

Network Type	public Internet
Measurement Type	Active measurement
Metrics	RTT, packet loss, topology, throughput
Sender Location	AARNet, Canberra, Australia
Receiver Location	Arizona State University, USA
Sender Platform	AMP Monitor, CPU 750MHz, Attached to 100Mb port of switch which is GbE attached to router (currently Cisco 7206VXR) The router currently has a dual unprotected STM1 to Pacific Wave (PNWGPOP) in Seattle
Receiver Platform	AMP Monitor, CPU 400MHz, connected to ASU High Speed Backbone via 100mb Ethernet
Timestamp Synch.	GPS
Number of Values	1440
Data Format	The RTT/Loss data is in the format of two columns. The first column is the seconds elapsed since the beginning of the start day your requested according to the pacific time zone and the second column is the round trip time or the word loss if it is a loss
Additional Info	The user can view the weekly and daily (including the current day) graphs of RTT, loss, IP hop count, jitter, and distribution of RTT. There are daily graphs for every day since measurement began. The graph for the current day is live.



Raw data



# MOME Database Model

Dataset name	RIPE NCC routing table, 01.02.2005, 00:00
Data type	Routing
File size	12.4MB
File compression	gz
Start time	2005-02-01 00:00:00
End time	2005-02-01 00:00:00
Duration	0:00:00
Description	Routing data from rrc00.ripe.net at RIPE NCC, Amsterdam. The data was captured on 01.02.2005, 00:00.
Dataset location	URL: <a href="http://data.ris.ripe.net/rrc00/2005.02/bview.20050201.0000.gz">http://data.ris.ripe.net/rrc00/2005.02/bview.20050201.0000.gz</a>
Tool	Zebra
Submitted by	mdabrowski @ 2005-02-04 10:36:47
Last Update	2005-02-04 10:36:47

Routing data



Raw data

# MOME Database Model

<b>Dataset name</b>	NASA-HTTP trace, July 1 to July 31, 1995
<b>Data type</b>	HTTP
<b>File size</b>	19.7MB
<b>File compression</b>	gz
<b>Start time</b>	1995-07-01 00:00:00
<b>End time</b>	1995-07-31 23:59:00
<b>Duration</b>	> 1 week
<b>Description</b>	One month's trace of all HTTP requests to the NASA Kennedy Space Center WWW server in Florida. Trace is stored in the Internet Traffic Archive
<b>Dataset location</b>	URL: <a href="ftp://ita.ee.lbl.gov/traces/NASA_access_log_Jul95.gz">ftp://ita.ee.lbl.gov/traces/NASA_access_log_Jul95.gz</a>
<b>Tool</b>	web server log

HTTP trace



Raw data

<b>Submitted by</b>	mdabro	<b>Collector Location</b>	NASA Kennedy Space Center WWW server, USA
<b>Last Update</b>	2005-02	<b>Filter Rules</b>	none
		<b>Trace Anonymisation</b>	none
		<b>Capture Platform</b>	web server log
		<b>Data Format</b>	The logs are an ASCII file with one line per request, with the following columns: host, timestamp, request, replay code, bytes in the replay.
		<b>Additional Info</b>	Timestamps have 1 second resolution.

# Outline

MOME

- | Short Intro – the MOME project
- | The MOME Database
  - | Meta-Data Approach
  - | MOME Trace Database
  - | MOME Tools Database
- | Automatic Analyses
- | Current Setup
- | Interfaces
  - | GUI, PUT/GET
- | Current Data
- | Outlook

# Automatic Analyses

- | Extract additional information from the raw data
- | Helpful for users who want to find interesting measurement data
- | Results stored in the MOME database as additional meta-data
- | Currently supported packet trace formats
  - | Libpcap (tcpdump)
  - | DAG (ERF)



**MOME** Cluster of European Projects  
aimed at Monitoring and Measurement

Information Society Technologies

Home > Database

About MOME  
Database  
Standardisation  
Publications  
Announcements  
Events  
Cluster Projects  
Related Sites  
Private Area

Logout "felix" Contact

Measurement Tools Measurement Data Statistics FAQ

Search Browse Add More Info

### MOME data analysis

Please choose the analysis tool from the list below. Remark, that each tool is applicable for specific data type and data format.

Basic analysis with 'tcpdstat' tool (**pcap**)  
Average traffic rate, packet interarrival time and packet size; histogram of packet sizes; bandwidth use per-protocol and per-application. Supported data type: **packet traces**. Supported data formats: **pcap (Ethernet)**.

Bit rate plots (**pcap**)  
Time-plots of bit rate, calculated over measurement intervals of different length. Supported data type: **packet traces**. Supported data formats: **pcap (Ethernet)**.

Bit rate plots (**erf**)  
Time-plots of bit rate, calculated over measurement intervals of different length. Supported data type: **packet traces**. Supported data formats: **erf (Ethernet)**.

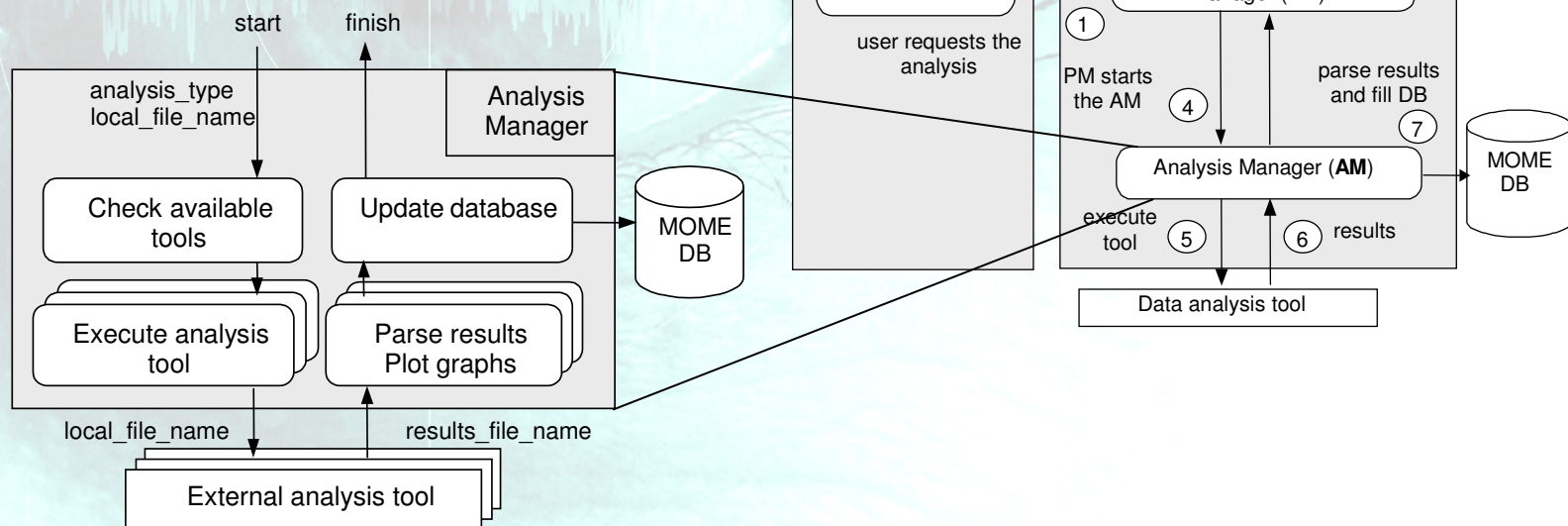
Bit rate plots (**tsh**)  
Time-plots of bit rate, calculated over measurement intervals of different length. Supported data type: **packet traces**. Supported data formats: **tsh**.

[Back to details](#)

Hosted by [TERENA](#)  
This page was last updated on Monday, May 22, 2006.

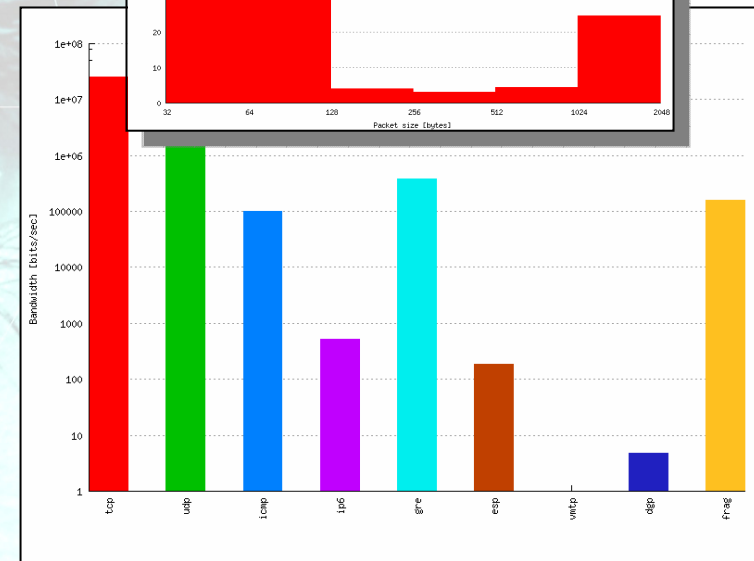
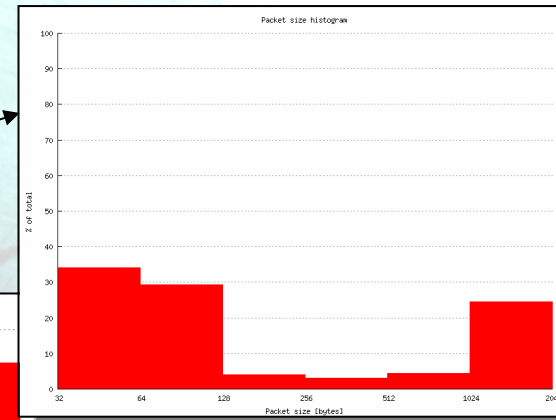
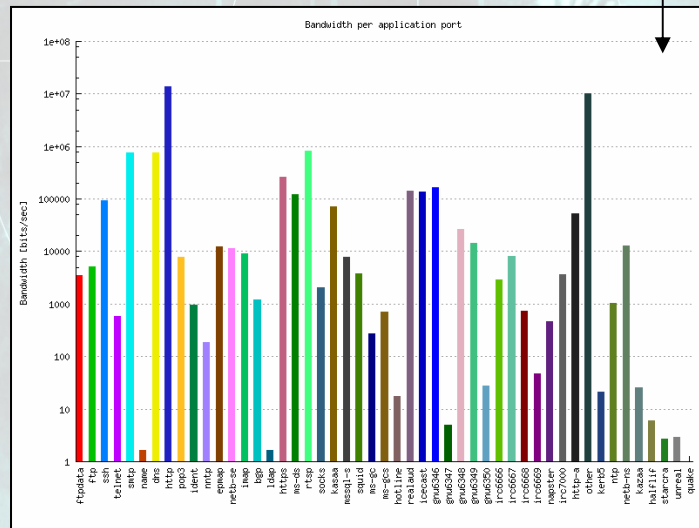
# Automatic Analyses

- | Open for incorporating new analysis tools
- | Available analysis results
  - | General statistics
  - | Bit rate plots

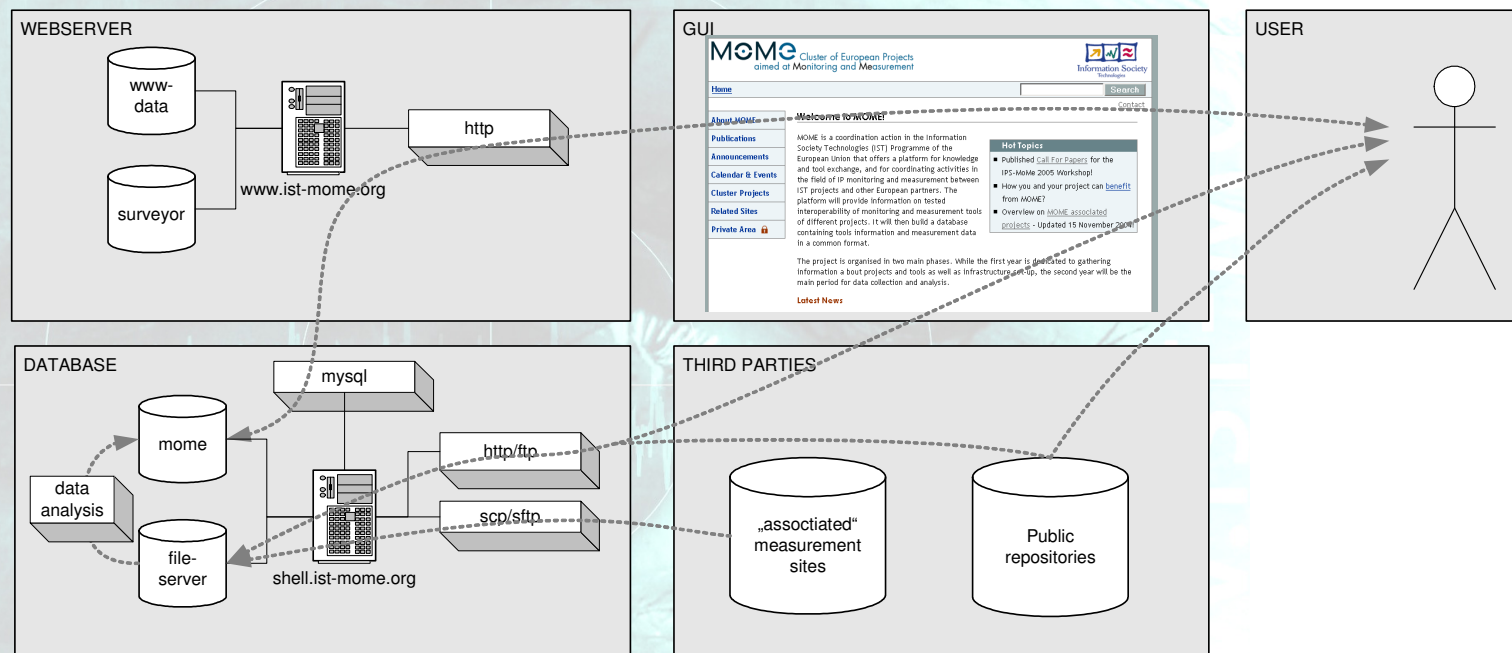


# Automatic Analyses - Example

Traffic rate, averaged over entire trace duration, in bit/s	27599219
Average packet inter-arrival time in sec	0.000131
Average packet size in bytes	452.9
Average packet arrival rate in pkt/sec	7616.76
Histogram of packet sizes	<a href="#">graph</a>
Bandwidth use per-protocol	<a href="#">graph</a>
Bandwidth use per-application	<a href="#">graph</a>



# Current Setup



# Interfaces

- | How to enter new meta-data to the database
  - | Web-GUI => "Add Dataset"
  - | Automatic "PUT"
    - | SFTP/FTP/SCP ASCII-File with meta-data
    - | Server-side script parses and puts data into database
    - | E.g. "FH-SBG..." Tracefiles
  - | Automatic "GET"
    - | Public repository provides Web-access
    - | "Crawler" takes meta-data from there
    - | E.g. "MAWI" Tracefiles

# Outline

- | Short Intro – the MOME project
- | The MOME Database
  - | Meta-Data Approach
  - | MOME Trace Database
  - | MOME Tools Database
- | Automatic Analyses
- | Current Setup
- | Interfaces
  - | GUI, PUT/GET
- | Current Data
- | Outlook

# Current Data



| Statistics page shows current amount of information



**MOME** Cluster of European Projects  
aimed at Monitoring and Measurement

Information Society Technologies

Home > Database

About MOME Login Register Contact

Database Measurement Tools Measurement Data Statistics FAQ

Standardisation

Publications

Announcements

Events

Cluster Projects

Related Sites

Private Area

### Database Statistics & Health Status

#### General Information

Number of registered users: 66  
Number of tool maintainers: 4  
Number of tool-maintainer associations: 4  
Number of tools: 123  
Number of data sets: 3706

#### Data Set Statistics

Total number of data sets: 3706  
Total size of data sets: 121.7GB

Number of packet traces: 3678  
Total size of packet traces: 121.7GB

Number of flow traces: 2  
Total size of flow traces: 16.8MB

Number of routing measurements: 1  
Total size of routing measurements: 12.4MB

Number of HTTP measurements: 1  
Total size of HTTP measurements: 19.7MB

Number of QoS measurements: 5  
Total size of QoS measurements: 65.5kB

Number of web repository measurements: 19  
Total size of web repository measurements:

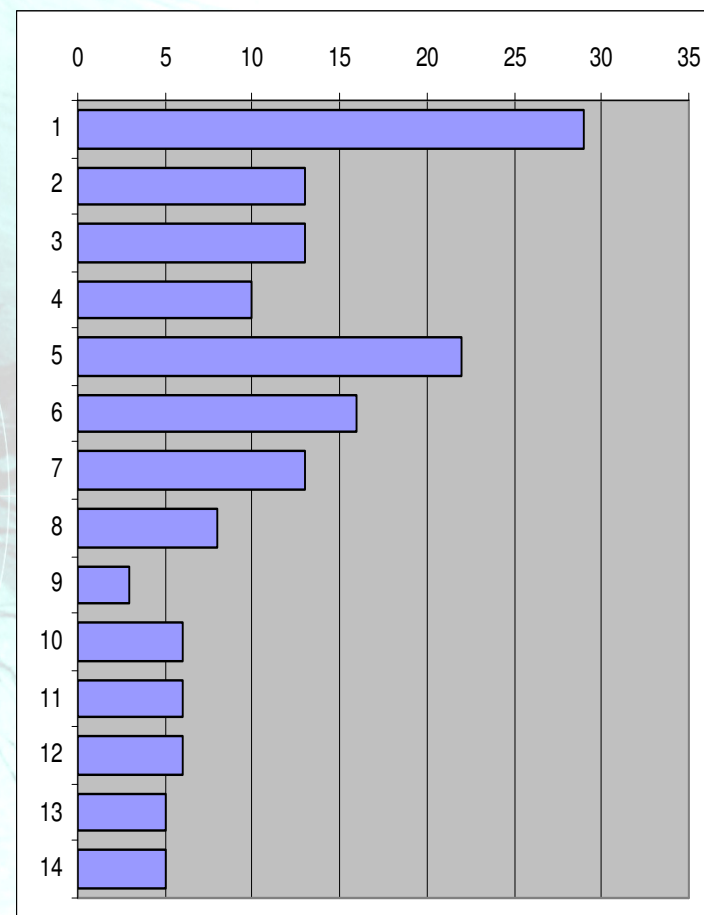
#### Data Base Health Status

Data base is ready.

Hosted by [TERENA](#)  
This page was last updated on Monday, May 22, 2006.

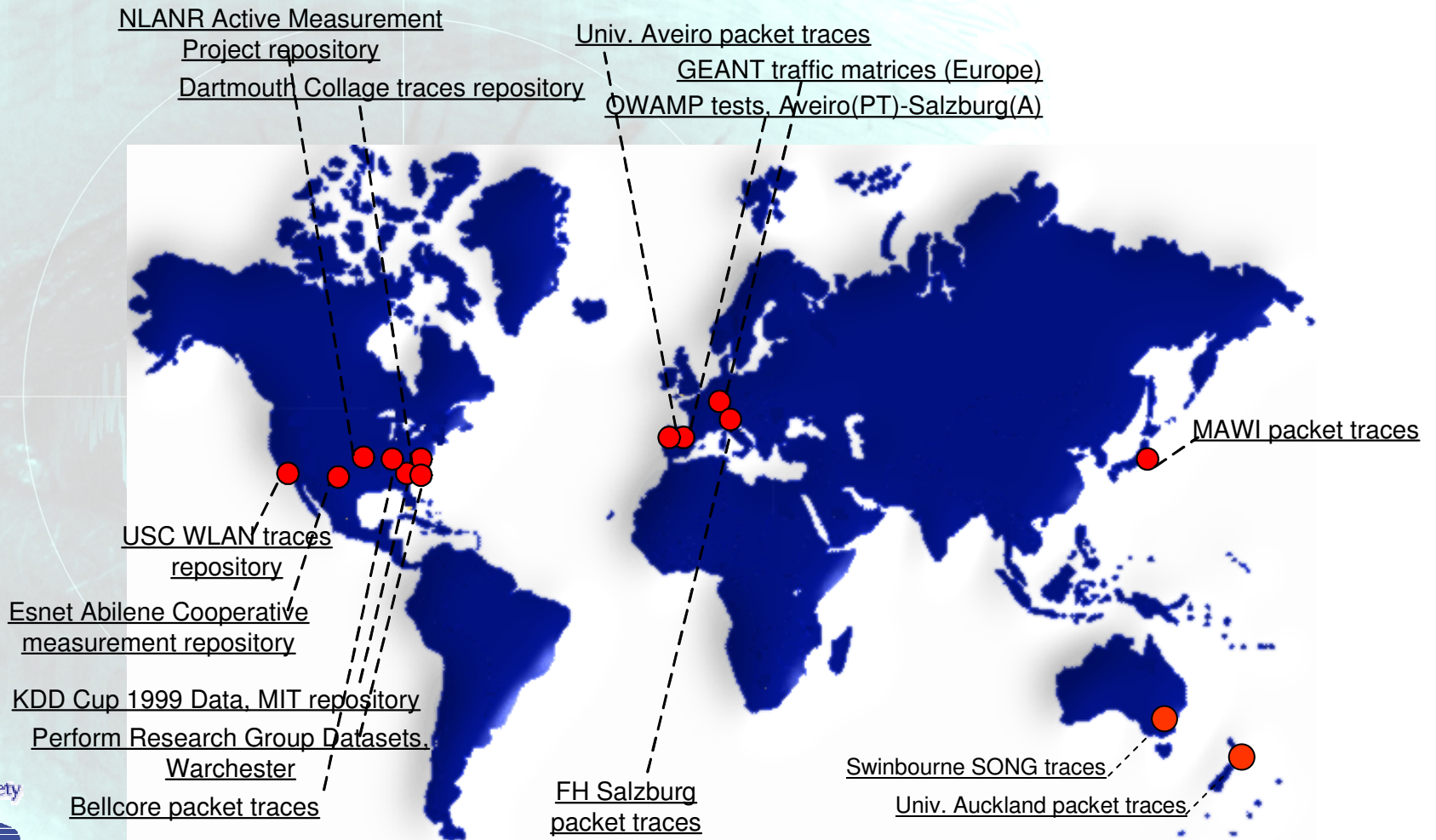
## Current Data – Measurement Tools

- | 123 Tools total
- | 29 '**Performance Measurement**'
- | 13 'Traffic Flow Measurement'
- | 13 'Packet Capturing'
- | 10 'Packet Monitoring'
- | 22 '**Connection Monitoring**'
- | 16 '**Traffic Visualization**'
- | 13 '**Route/Topology Detection**'
- | 8 'Traffic Generation'
- | 3 'Application-level Monitoring'
- | 6 'Accounting'
- | 6 'Bandwidth Measurement'
- | 6 'Service Monitoring'
- | 5 'Intrusion Detection'
- | 5 'Sniffing'



| many tools belong to more than one category

# Current Data – Measurement Traces



## Outlook

- | MOME project ended March 2006
- | Web-page and Database stays online
  - | Hosted by TERENA
- | Database still maintained by
  - | Salzburg Research
  - | Fraunhofer FOKUS
  - | Warsaw University of Technology
- | Improvement capabilities are there
- | Follow-up projects under discussion
  - | FP7
  - | Others
- | Co-operation with CAIDA IMDC desired
- | Further co-operation is kindly welcome!!!

**Thank you for your attention!  
Questions?**

**MOME**

Felix Strohmeier  
Salzburg Research  
Jakob-Haringer-Str. 5/III  
A-5020 Salzburg  
Tel: +43/662/2288-443

[felix.strohmeier@salzburgresearch.at](mailto:felix.strohmeier@salzburgresearch.at)  
<http://www.salzburgresearch.at>  
<http://www.ist-mome.org>

