
Tango plugin for Etherreal

Paolo Frigo - paolo.frigo@elettra.trieste.it



What is Ethereal?

The world's most popular network protocol analyzer. It's open source and runs on Unix, Linux and Windows platforms.

Tango plugin Develop

Tango Meeting
26-27/05/2005



Requirements:

- Ethereal source code
- tango.idl
- idl2eth

Plugin develop:



Build Ethereal with the packet-tango.c and the modified Makefiles

Ethereal with the new plugin

Tango Meeting
26-27/05/2005



Let's try out all Ethereal capabilities to analyse TANGO traffic...

	Source	Destination	Protocol	Info
9197	192.168.205.50	192.168.204.50	TANGO	GIOP 1.2 Request 2968654: comr
0343	192.168.204.50	192.168.205.50	TANGO	GIOP 1.2 Reply 2968654: No Exce
0694	192.168.205.50	192.168.204.50	TANGO	GIOP 1.2 Request 2968656: comr
1197	192.168.204.50	192.168.205.50	TANGO	GIOP 1.2 Reply 2968656: No Exce
3928	192.168.205.50	192.168.204.50	TANGO	GIOP 1.2 Request 2968658: comr
5012	192.168.204.50	192.168.205.50	TANGO	GIOP 1.2 Reply 2968658: No Exce
5405	192.168.205.50	192.168.204.50	TANGO	GIOP 1.2 Request 2968660: comr
5859	192.168.204.50	192.168.205.50	TANGO	GIOP 1.2 Reply 2968660: No Exce
4107	192.168.205.50	192.168.205.195	GIOP	GIOP 1.2 Request 342: push_struc

TANGO Details

- General Inter-ORB Protocol
- General Inter-ORB Protocol Request
- Cosnaming Dissector Using GIOP API
- Coseventcomm Dissector Using GIOP API
- Tango Dissector Using GIOP API
 - length = 6
 - command = State
 - TypeCode enum: tk_null (0)
 - Enum value = 2 (CACHE_DEV)

Packet Bytes

```
00a0 00 00 00 00 00 00 01 d9 bb e1 dc aa b1 30 00 00 .....0..
00b0 00 00 00 00 00 00 00 00 00 00 00 00 06 53 74 .....St
00c0 61 74 65 00 00 00 00 00 00 00 00 00 02 ate.....
```

Ethereal with the new plugin

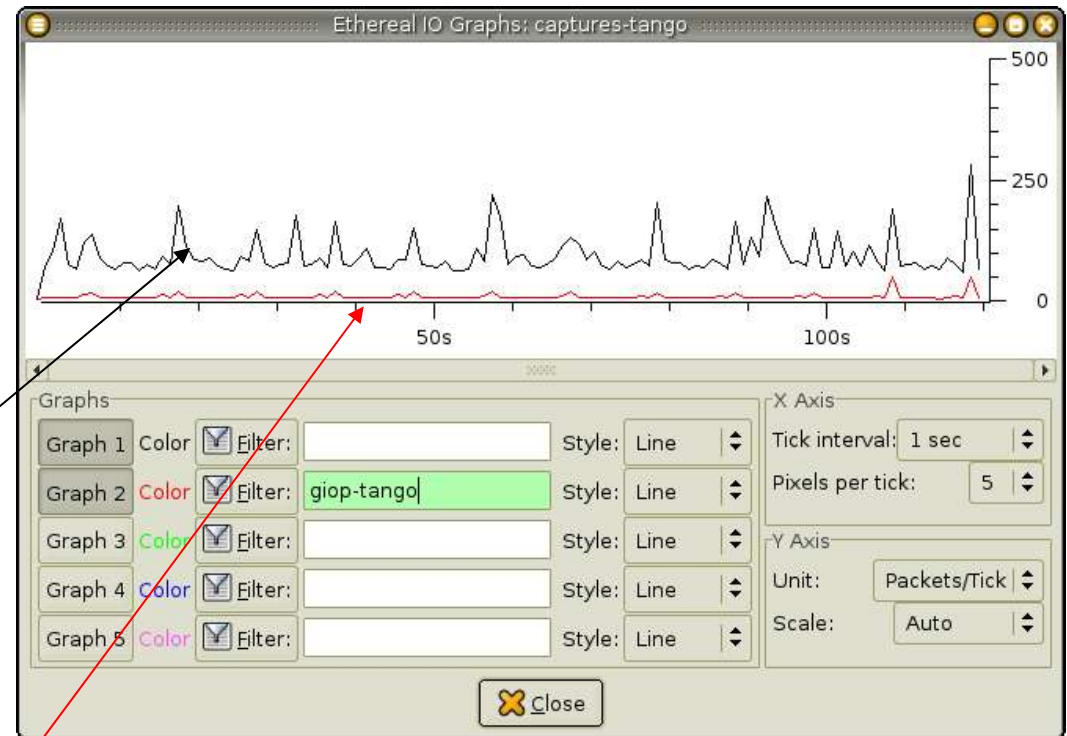
Tango Meeting
26-27/05/2005



Ethereal also generates interesting statistics:

- ✓Summary
- ✓Protocol Hierarchy
- ✓Conversation
- ✓Endpoints
- ✓IO Graphs

e.g. Traffic - Packets/Seconds



All network traffic

Tango Traffic

Ethereal plugin

Tango Meeting
26-27/05/2005



Ethereal developers are considering whether to include the TANGO plugin in the official release.

<http://www.elettra.trieste.it/~tango/>