



RE-IMPLEMENTATION AND GRAPHICAL ENHANCEMENT OF THE INETVIS VISUALISATION TOOL

By: Christopher Schwagele
Supervisor: Barry Irwin



RHODES UNIVERSITY
Where leaders learn

PRESENTATION OUTLINE

1. InetVis Tool

- Quick Recap

2. Progress

- Client-Server model
- Server Progress
- Client Progress

3. Issues

- OpenGL (OpenTK) and XNA
- WinForms and XNA
 - XNA within WinForms
 - WinForms within XNA

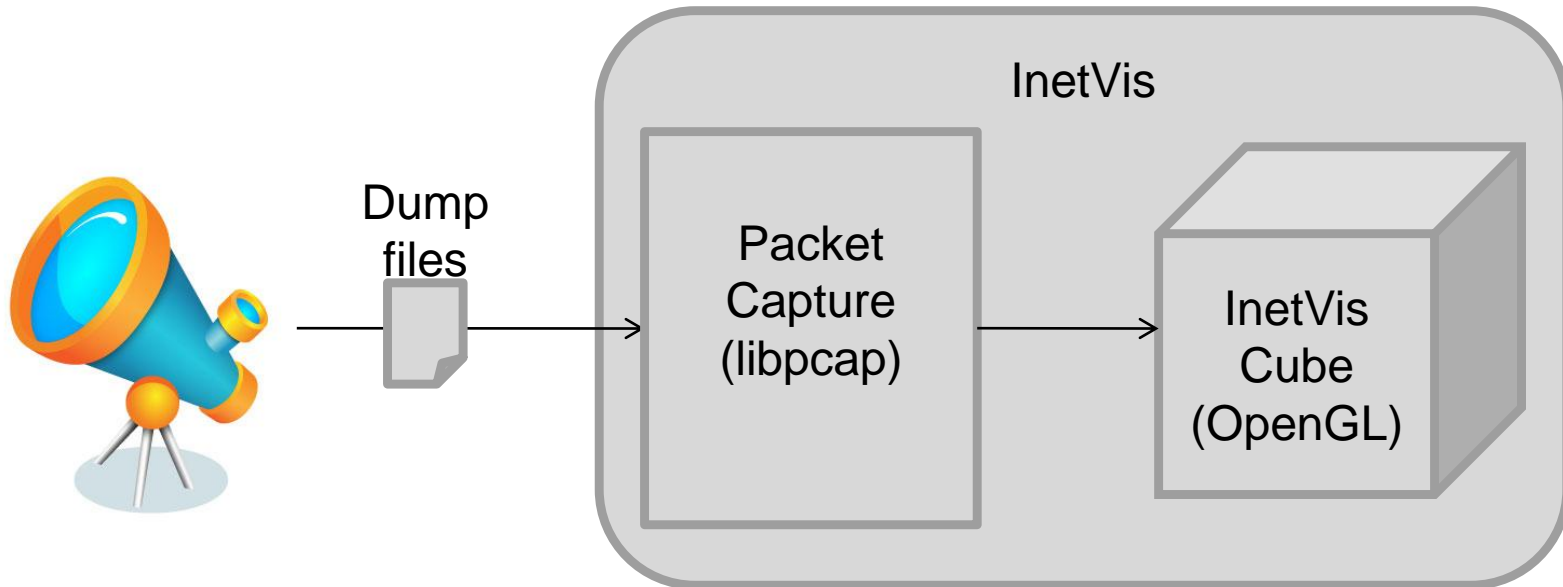
4. Remaining Work

- Network Interface
 - dVP
- Playback
 - Packet Information
 - aviFile library

1. INETVIS TOOL

Quick Recap

- 2 components
 - Packet Capture
 - Animated 3D scatter plot cube



Screenshot

1. INETVIS TOOL

Plotter Settings

Plotting

Destination Home Network Range (Blue x-Axis)
0 . 0 . 0 . 0 / 0 Guess ✓
0.0.0.0 - 255.255.255.255 (0.0.0.0)

Source Internet Network Range (Red z-Axis)
0 . 0 . 0 . 0 / 0 Full Range ✓
0.0.0.0 - 255.255.255.255 (0.0.0.0)

PortRange (Green y-Axis)
0 - 65535 ● linear plot ○ log plot 100 ✓

Colour Mapping

scheme Destination port

Background
○ white ● black □ transparent decay

Points
size 2
□ smooth
□ bulge

Reference Frame Settings

Projection Mode
● perspective
○ orthographic

Transparent Grid
□ front
□ back
□ left
□ right
□ top
□ bottom
□ plane
Opacity 20

Reference Frame
☒ primary axes
☒ bounding axes
☒ TCP/UDP cube
☒ ICMP plane
□ markers

Grid Partitions
blue x-axis (destination home network): 10
red z-axis (source internet network range): 10
green y-axis (port range): 10

Text Labels
☒ axis ☒ date & time □ framerate

InetVis Control Panel

File Mode Replay Record View Help

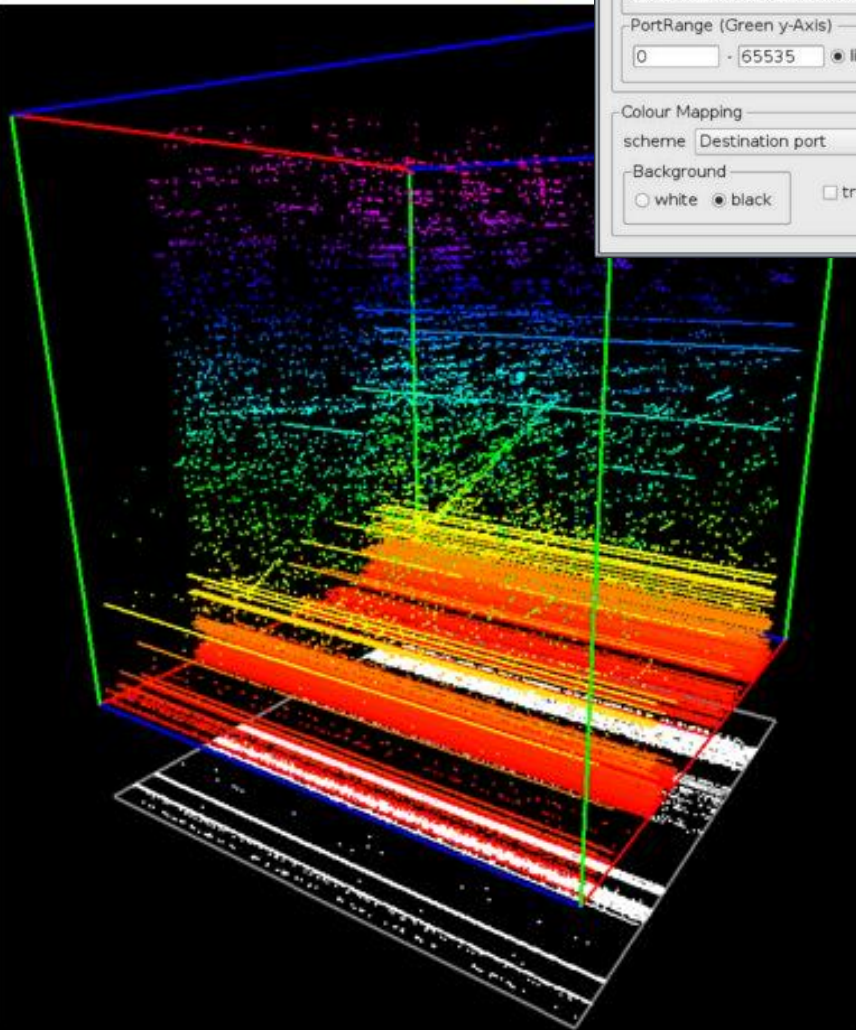
Replay Position
24/08/2005 21:30:56 323 ✓ 0

Replay Speed
▶ time scale 1 x Record

Historic View
time window 1 00:00:00 0 ✓

Filter
BPF expression

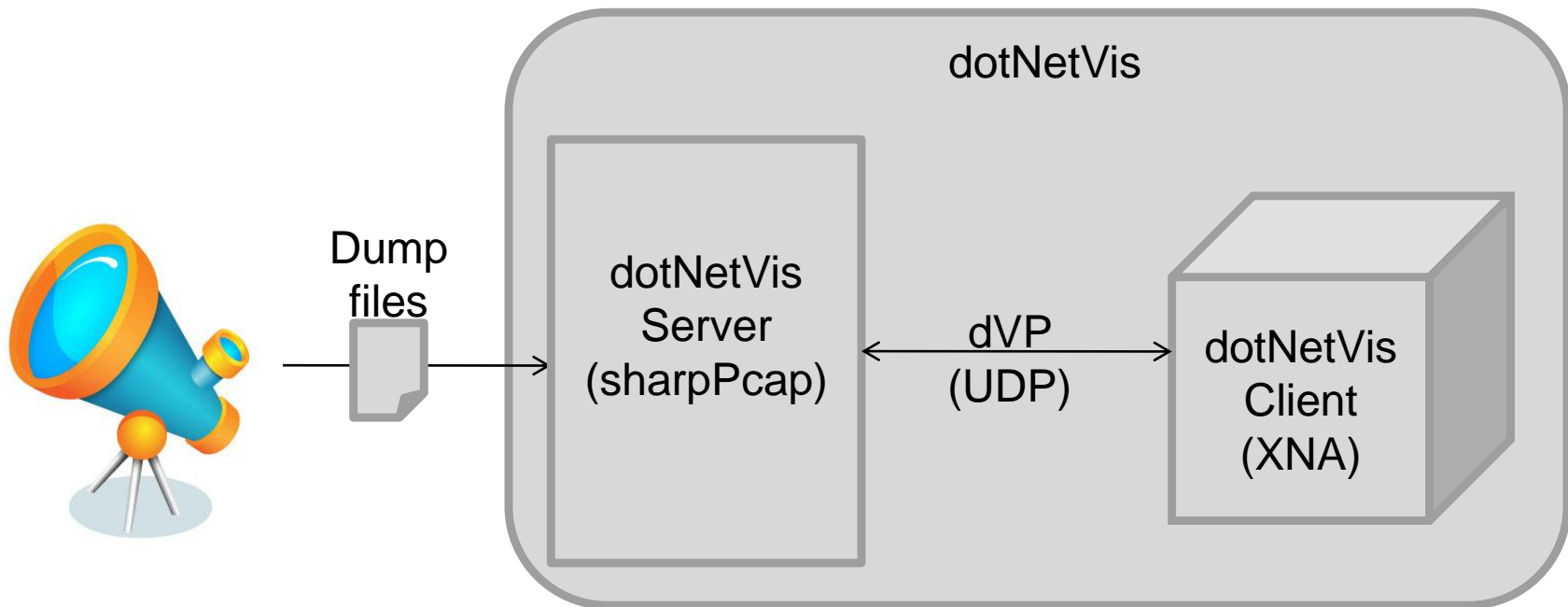
Event buffer: 10



2. PROGRESS

Client-Server model

- dotNetVis Client
- dotNetVis Server
- Intercommunication



dotNetVis Server Progress

- SharpPcap working nicely
- Example tutorials
- Live capture through local network adapter

dotNetVis Client Progress

- Cube draws!
- GUI structure complete
- Skeleton outline complete
 - Array of Vector3 objects to represent packets
 - Array is plotted in cube

dVP

- ???



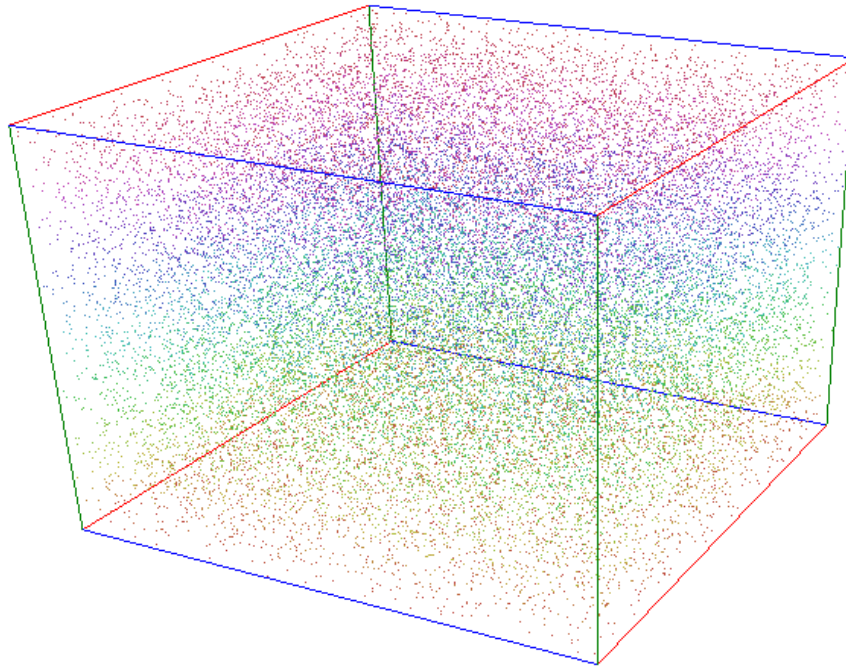
3. ISSUES

OpenGL, OpenTK and XNA

- OpenTK – missing functionality
- OpenGL vs XNA...

WinForms and XNA

- Nightmare!
- Why compatibility issues?
 - WinForms – event driven
 - XNA - polling
- XNA within WinForms
- WinForms within XNA
 - How?
 - Problems
 - Line and Point width
 - Keyboard input
 - Custom Control
 - How does it compare with InetVis?



but
ton
7

4. REMAINING WORK

dotNetVis Server

- Read dump files
- Network interface with dVP support

dotNetVis Client

- InetVis functionality
 - Record to AVI file
 - aviFile library
 - Variable time playback
- Network interface with dVP support
- Packet Information by ID

THE END



QUESTIONS?

Presented By: Christopher Schwagele