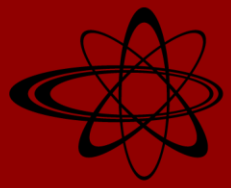


SNRG
Security and Networks Research Group

ENHANCEMENT AND RE-IMPLEMENTATION OF THE INETVIS VISUALISATION TOOL

By: Christopher Schwagele
Supervisor: Mr Barry Irwin

Telkom
amatole telecommunication services
Bright Ideas 39
STORTECH For Your Information
THRIP Technology and Human Resources for Industry Programme
COMVERSE
tellabs

RHODES UNIVERSITY
Where leaders learn

PRESENTATION OUTLINE

Presentation Outline

1. Background

- Definitions
- InetVis Visualisation Tool
- Project Objectives

2. Main Differences

- Underlying Model

3. dotNetVis Server

- Packet Processing

4. dotNetVis Client

- Structure
- Visualisation

5. dotNetVis Communication

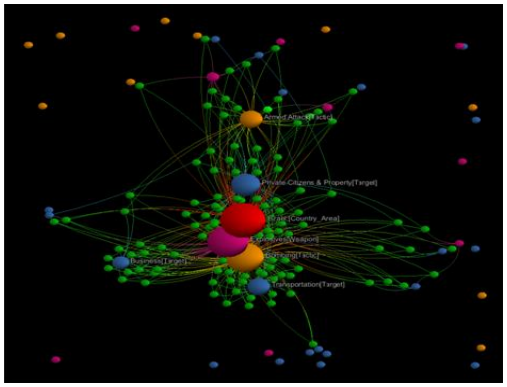
- Protocol
- Library
- API

6. Extensions

1. BACKGROUND

Definitions

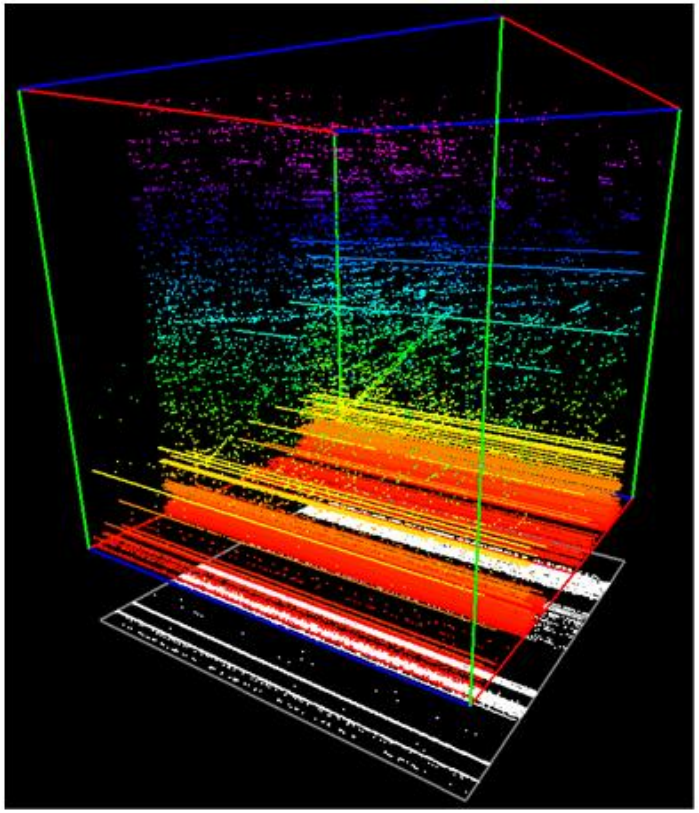
- Data Visualisation
  - Purpose
  - Process

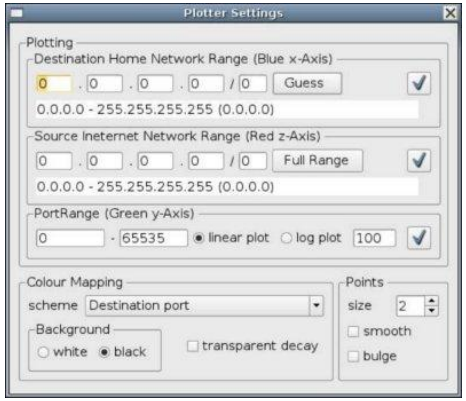


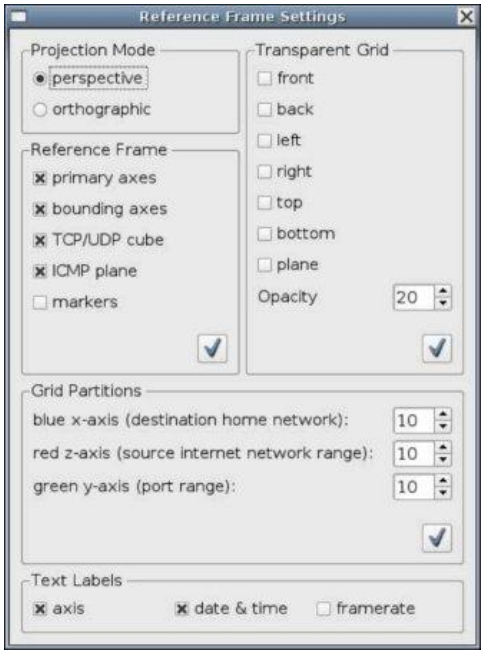
- Network Telescope
  - Purpose
  - Output

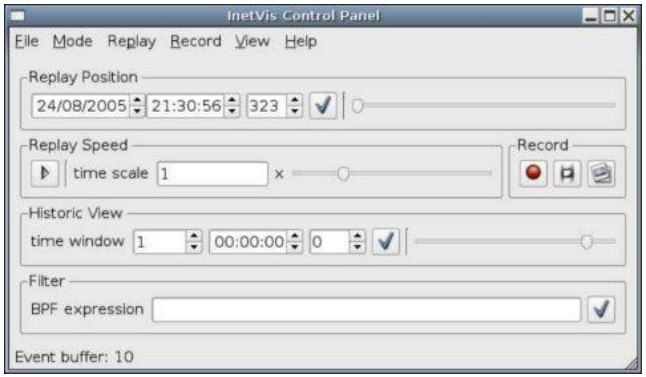
InetVis Visualisation Tool

- Master's Project – J.P. van Riel
- Underlying Architecture
- Packet Capture - libpcap
- Rendering – OpenGL
- Performance









Security and Networks Research Group

Rhodes University
Where leaders learn

Project Objectives

- Problem Statement
- InetVis short-fallings
- Proposed Enhancements
  - Separating the components
  - Exploiting parallel processing
  - Enhancing the GUI
  - Immersive packet navigation
- Porting the system
  - dotNetVis

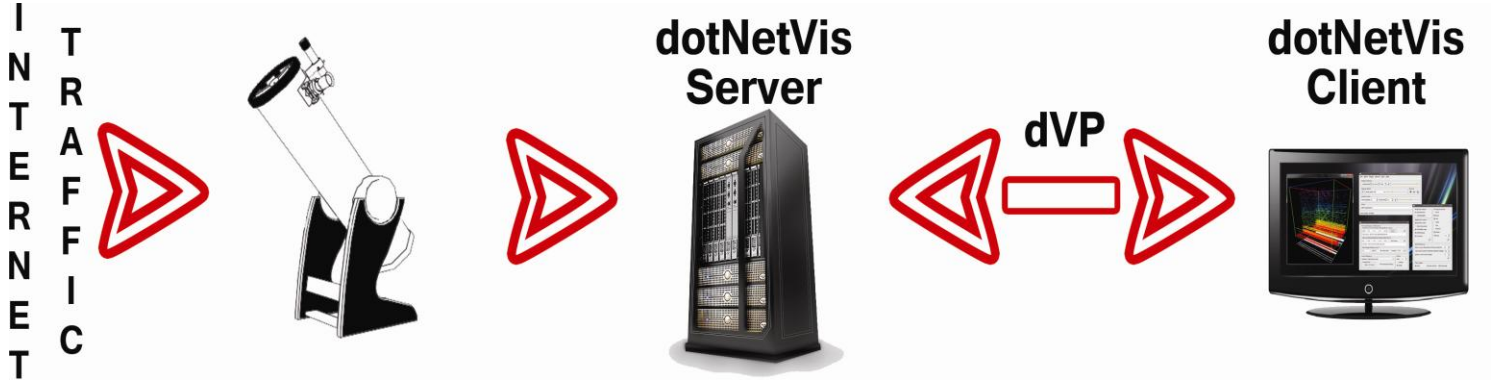
2. MAIN DIFFERENCES

Development

- Environment
  - .NET vs. C++
  - XNA, openGL, openTK??

Underlying Model

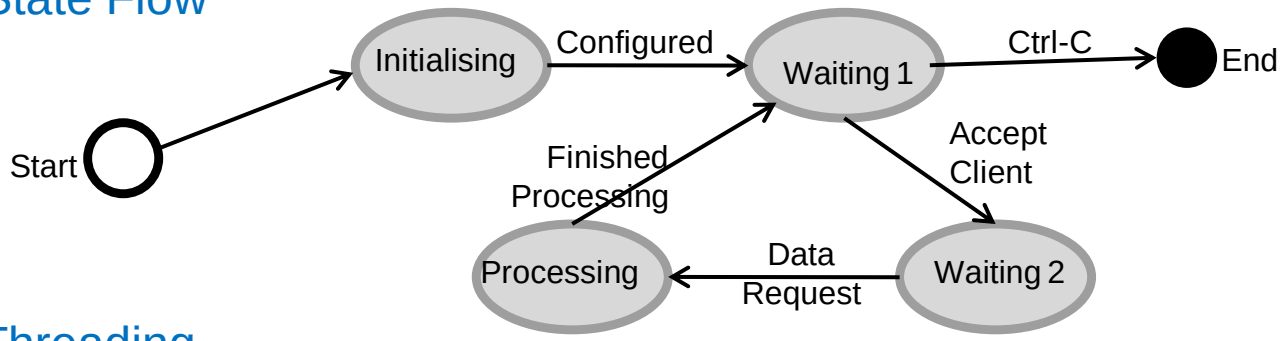
- **Client Server Model**
  - Modularization
    - Processing
    - Memory
  - Flexibility
    - Future Implementations
    - Generic Communication – dotNetVis Protocol (dVP)



3. DOTNETVIS SERVER

Structure

- Main Program
- Packet Processing Component
  - SharpPcap
- Communication Component
  - dVP (dotNetVis Protocol)
- State Flow



- Threading

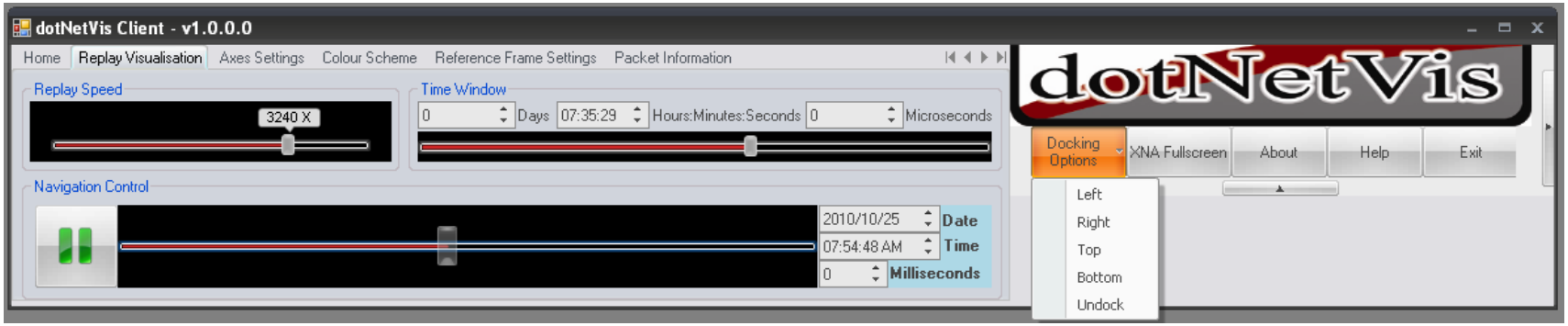
Packet Capture

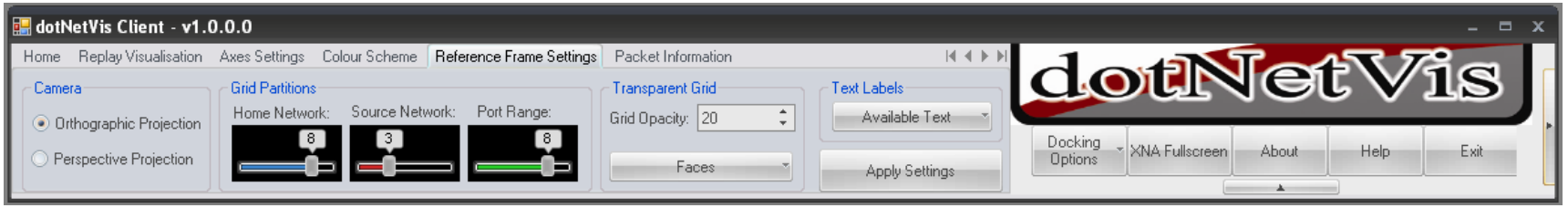
- Capture Device Selection
- Capturing packets from a Device
- Processing Packets
- Processing Termination

3. DOTNETVIS CLIENT

Structure

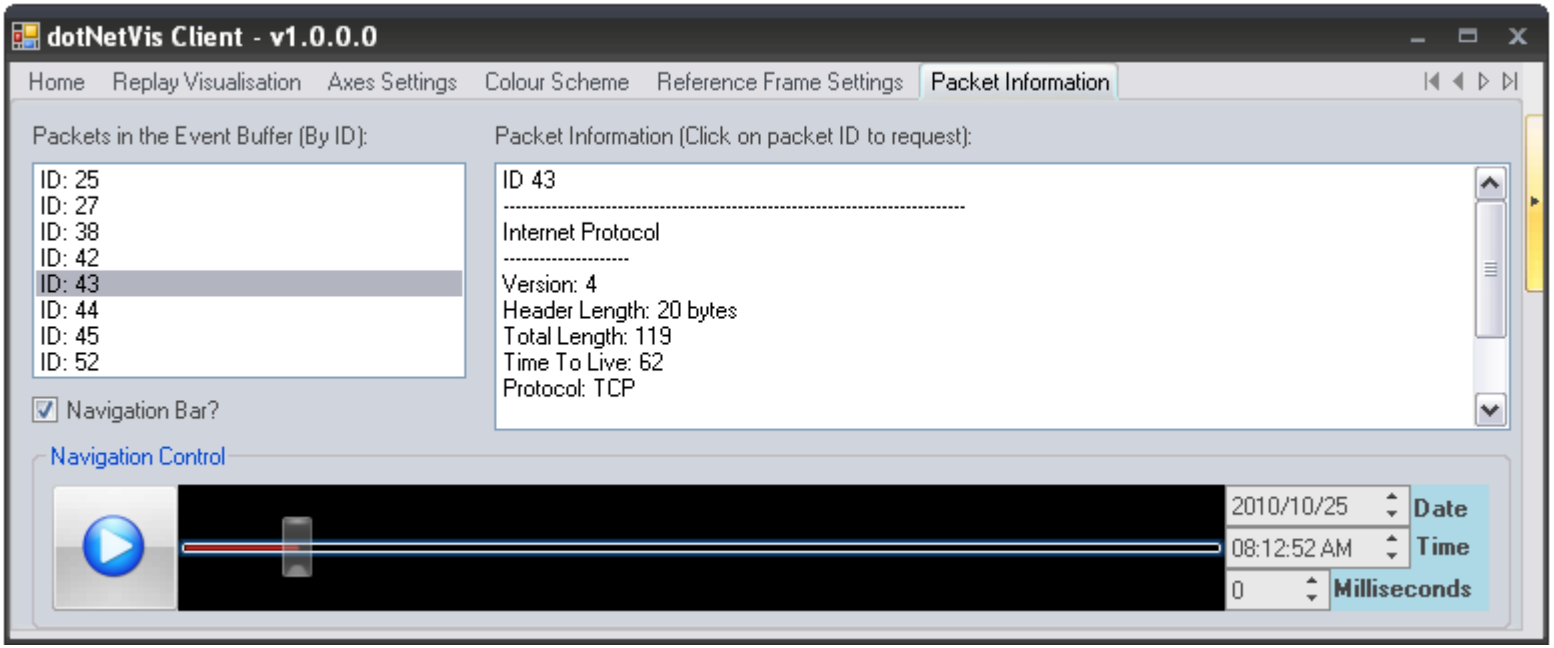
- Component Manager
  - Threading
- Visualisation Component
  - XNA and WinForms: Relationship Issues… (Can't escape them!)
  - Solution?
  - Implementation
- Settings Component



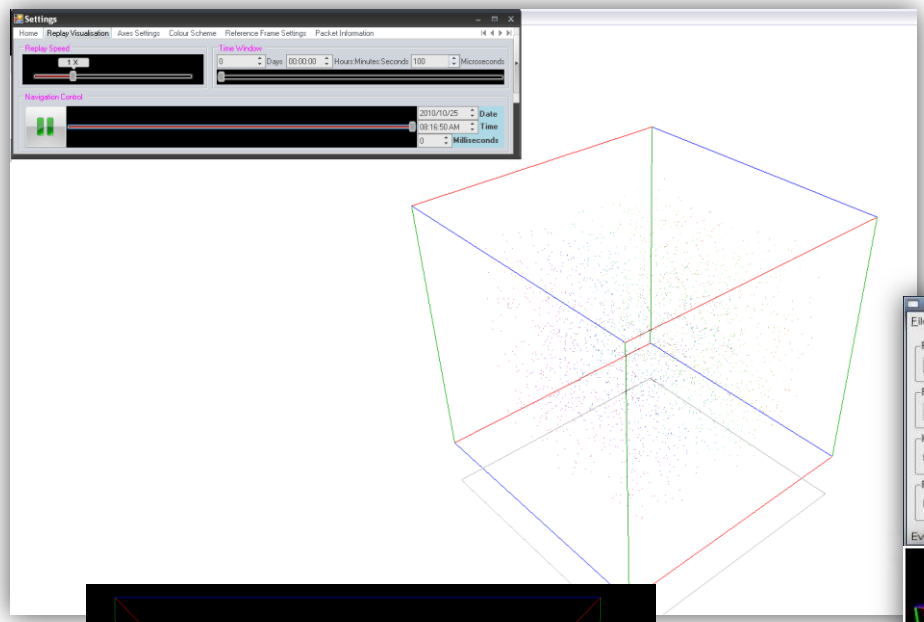


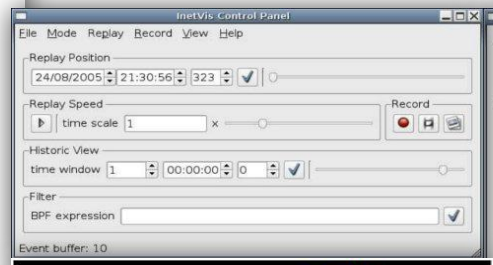
Settings (contd.)

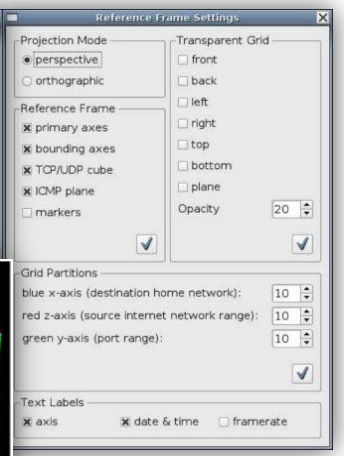
- Changing settings
- Packet Selection
  - Cube point highlighting
  - Packet Information

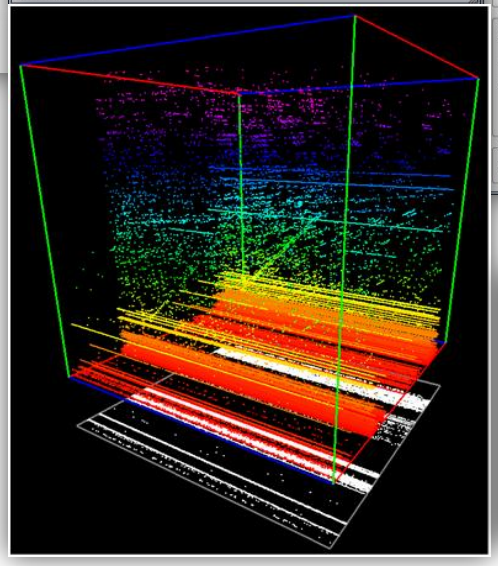


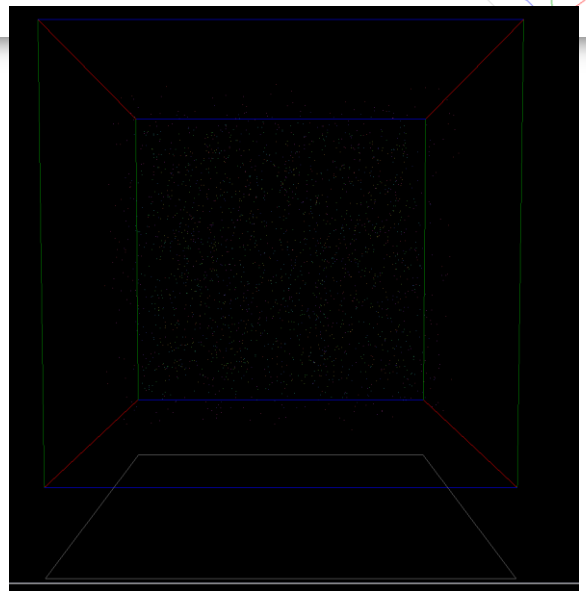
Comparison of screen consumption

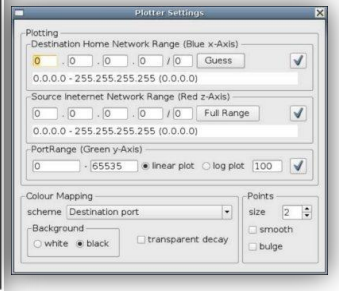










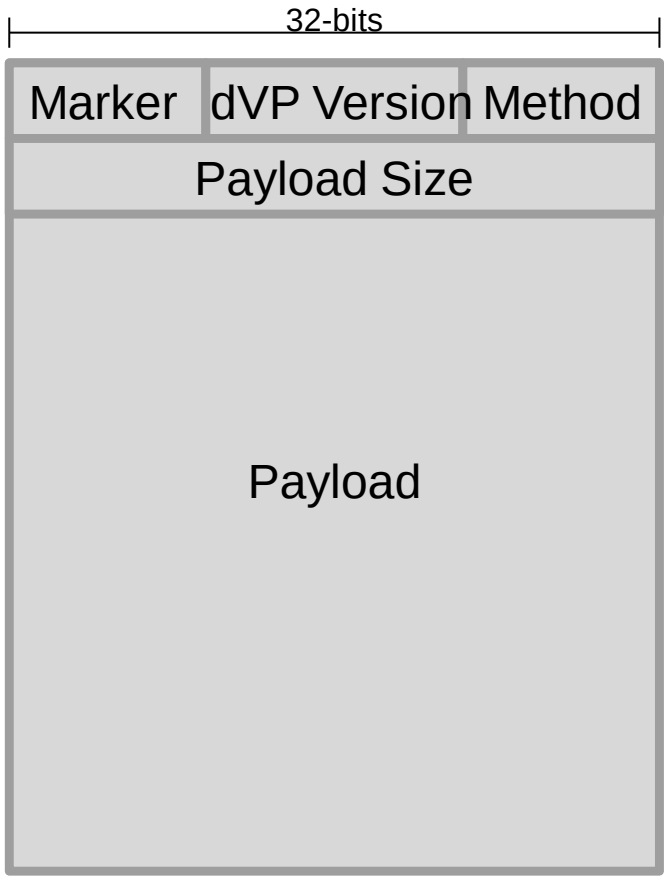


4. DOTNETVIS COMMUNICATION

Protocol (dVP)

- Necessity
- Packet transport - TCP
- Packet Structure

- Methods
  - Requests
  - Responses



Library

- **Transmitter**
- **Receiver**

- **Communication Channel Initialisation**
  - TCP connection
  - Data Streams

- **dVP Packet creation**

- **Sending data**
- **Receiving data**
  - Identification
  - Worker Thread Utilisation
  - Storage
  - List indexing

- **Point3D custom-defined struct**

API

- **Sending data**
  - Transmit()
    - Packets
    - Status messages
- **Retrieval of stored data**
  - Initial retrieval
  - Retrieval using indeces
- **Flexibility**
  - Usage of API
  - Data Types

6. EXTENSIONS

Less complex

- Colour schemes and legends
- Intelligent reference frames
- Capture file playlist with queing
- Client side packet filtering

More complex

- Intrusion detection through intelligent pattern analysis
- Range of graph types

- Evolving dVP components into a flexible visualisation framework

THE END

QUESTIONS?

Presented By: Christopher Schwagele