NetVis

Network Security Visualisation Tool

Sponsor: Jassim Happa, University of Oxford

Developers: James Nicholls, Dominik Peters, Albert Slawinski, Thomas Spoor, Sergiu Vicol

Project Goals

Implement an application to assist an **observer** in the detection of potential network attacks.

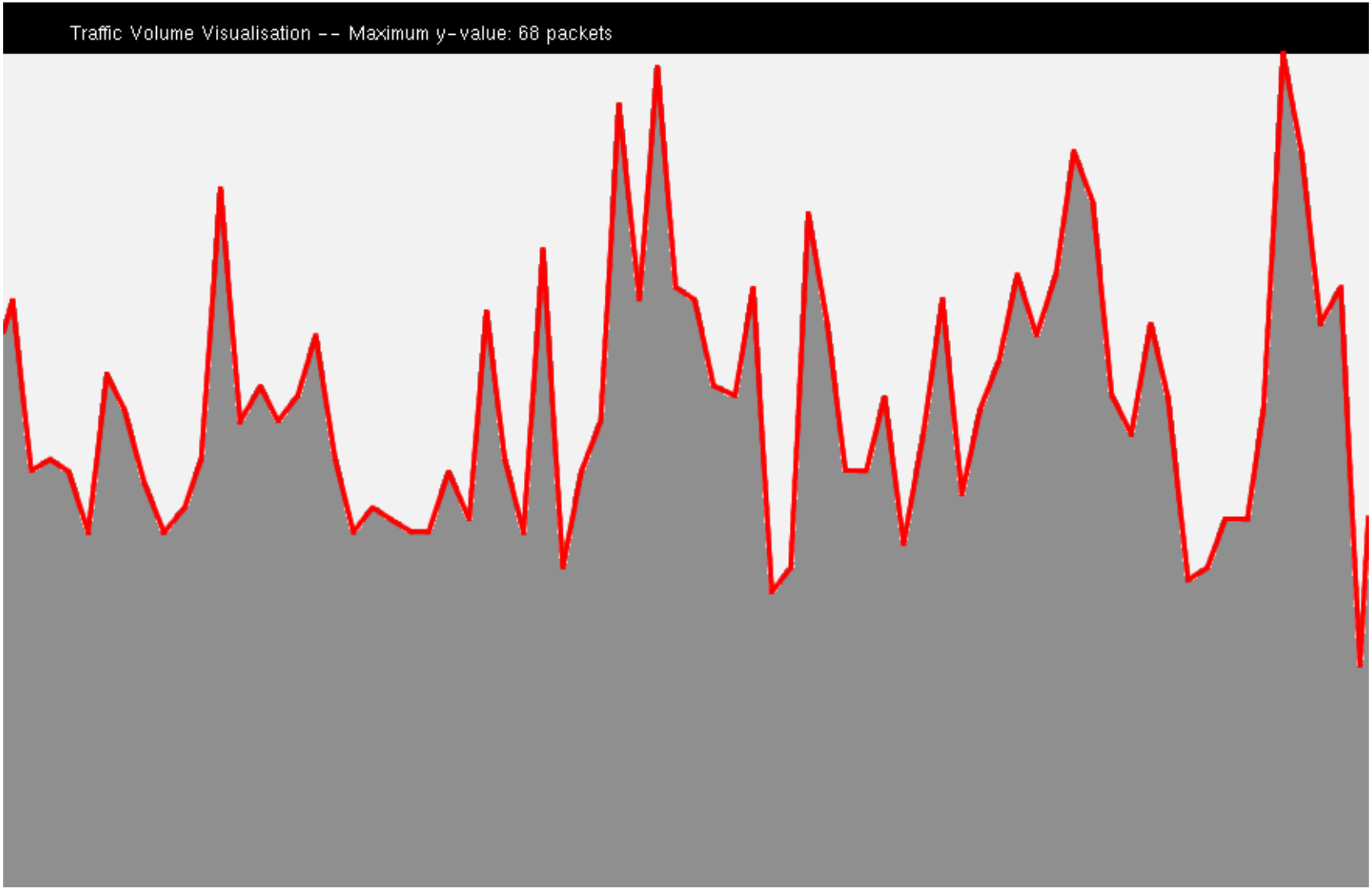
Improve situational awareness of a network faster than automated analytical techniques (i.e. using an IDS).

Design Choices

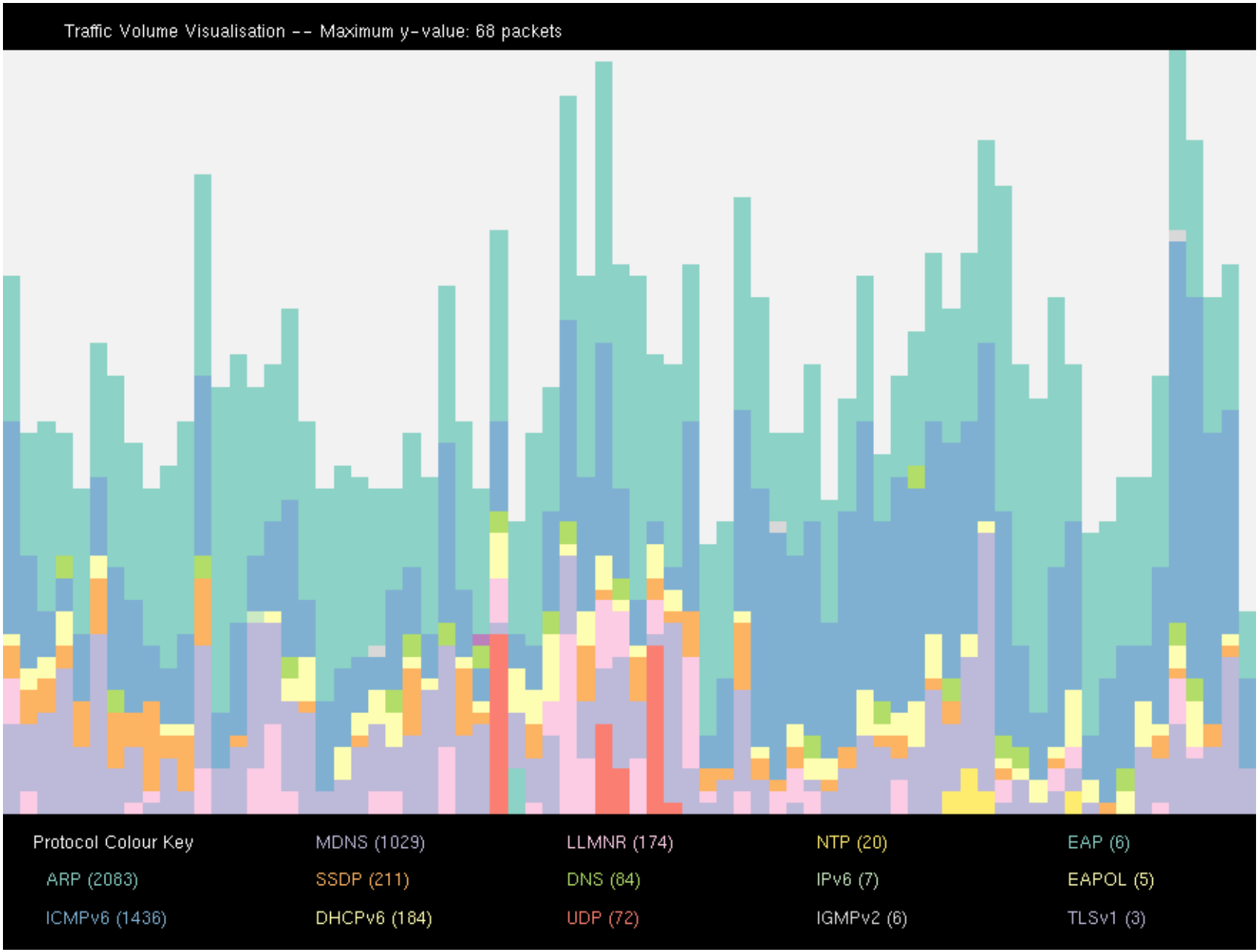
The decisions we made in the early stages of the project;

- Java / Swing / OpenGL graphics API
- Network "map" for familiarity
- Overview $\rightarrow$ zoom and filter $\rightarrow$ details on demand [Shneiderman, 1996]
- Variety of visual styles

An unhelpful visualisation



A better visualisation

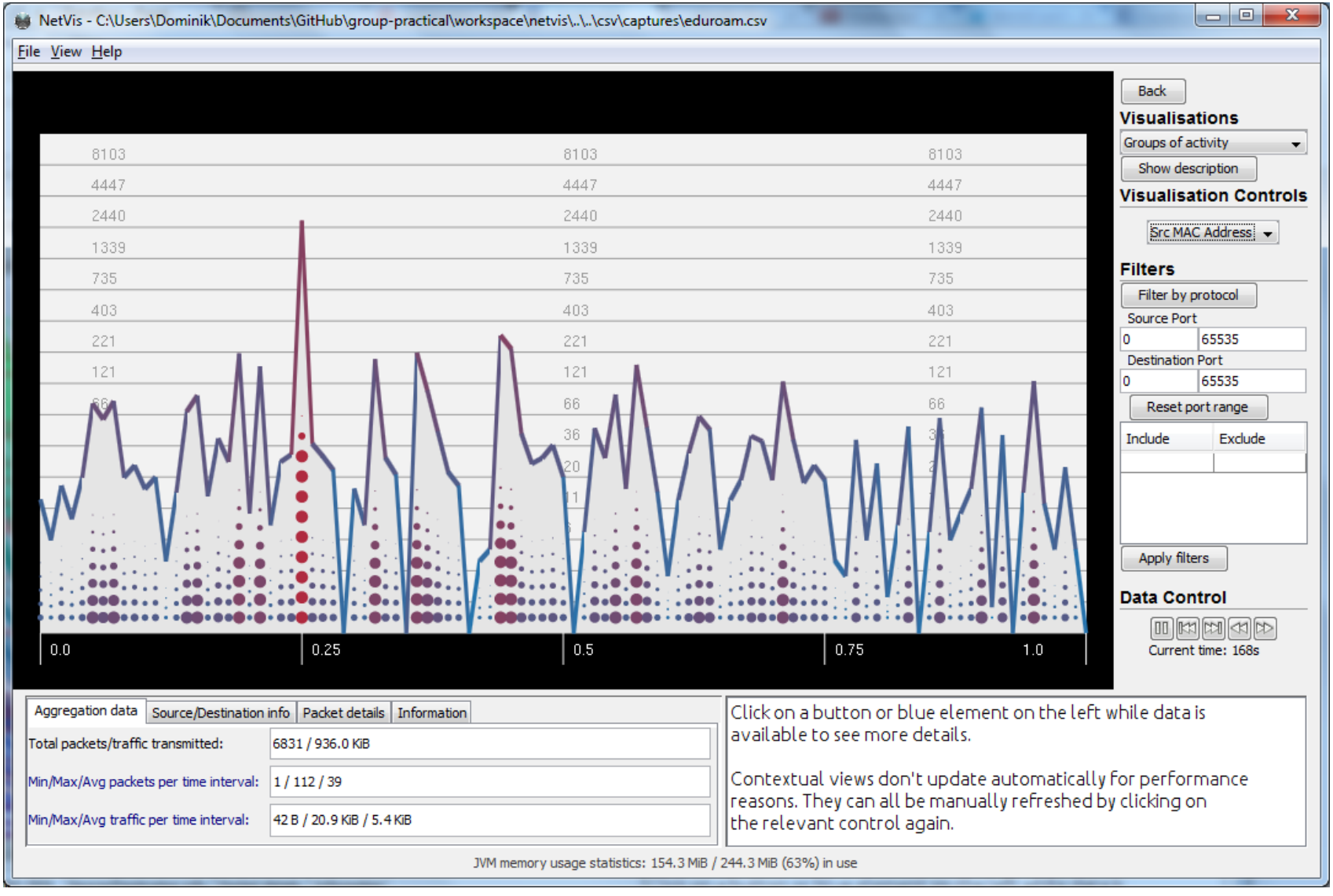


Teamwork

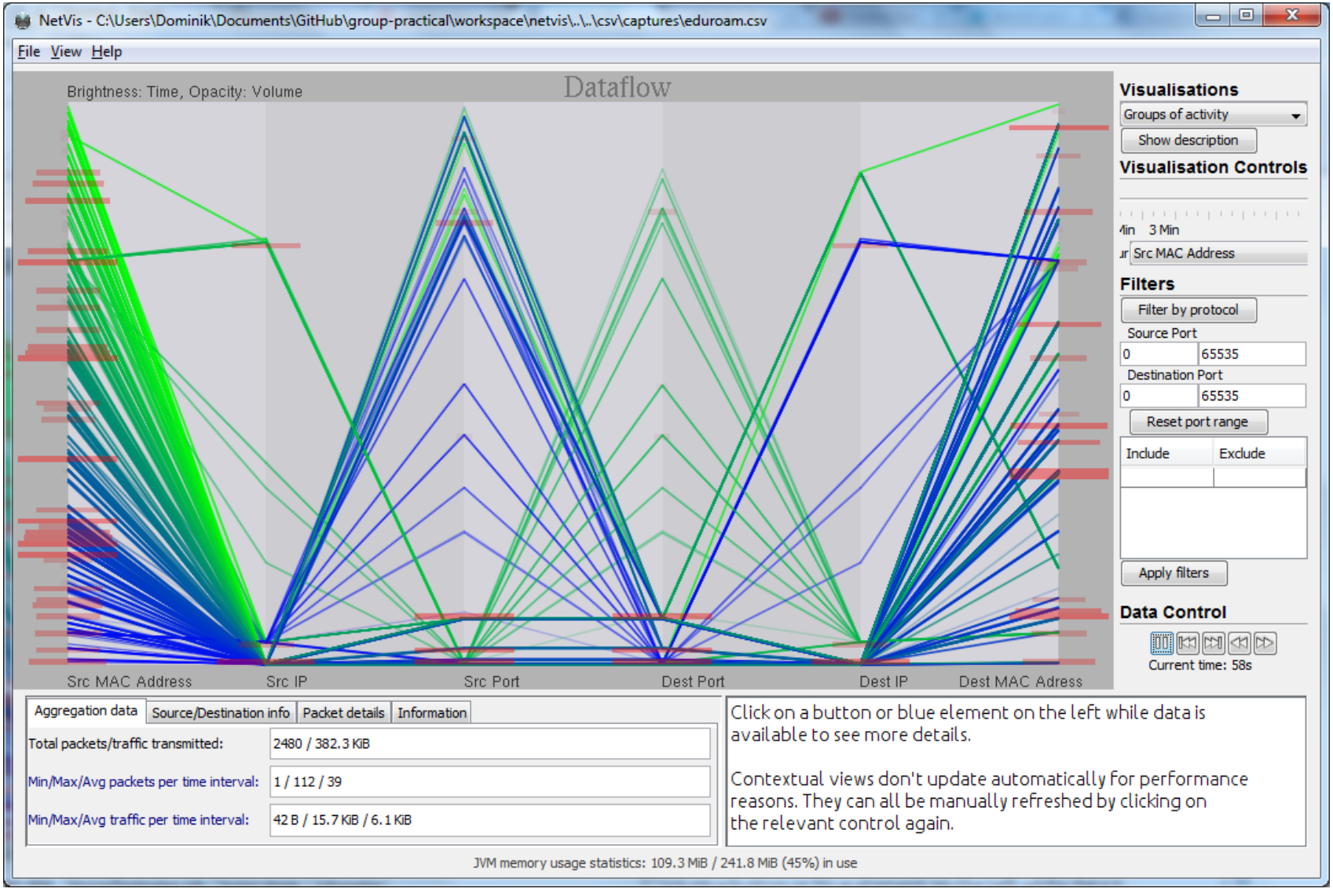
Tools used to promote Synergy^{TM} between team members

- Version control, code hosting: **GitHub**
- Distribution of tasks: **Google Drive**, **GitHub**
- Meeting planning: **Facebook**, **Doodle**
- Shouting at people: **Facebook**, **GitHub**

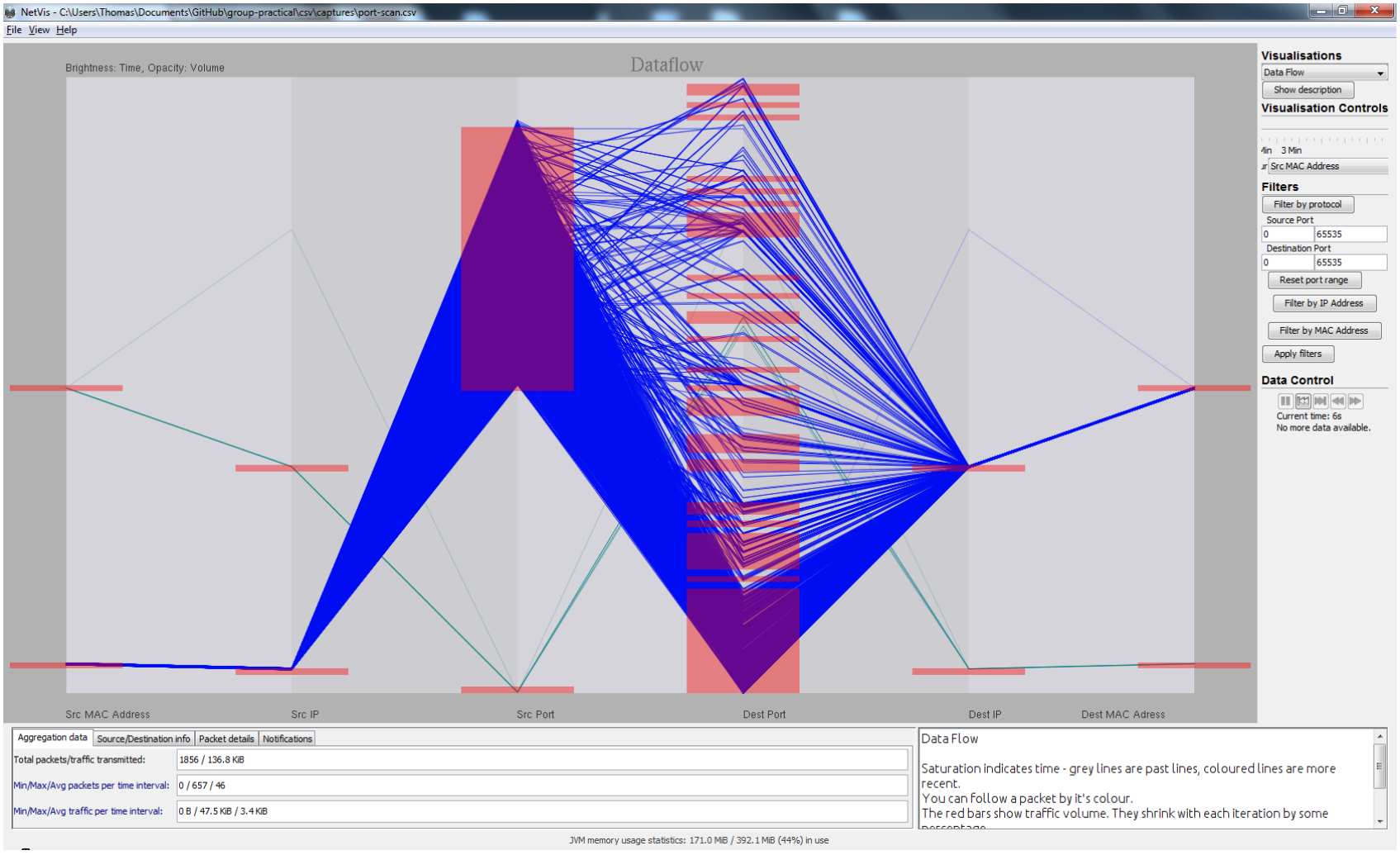
Attributes Visualisation



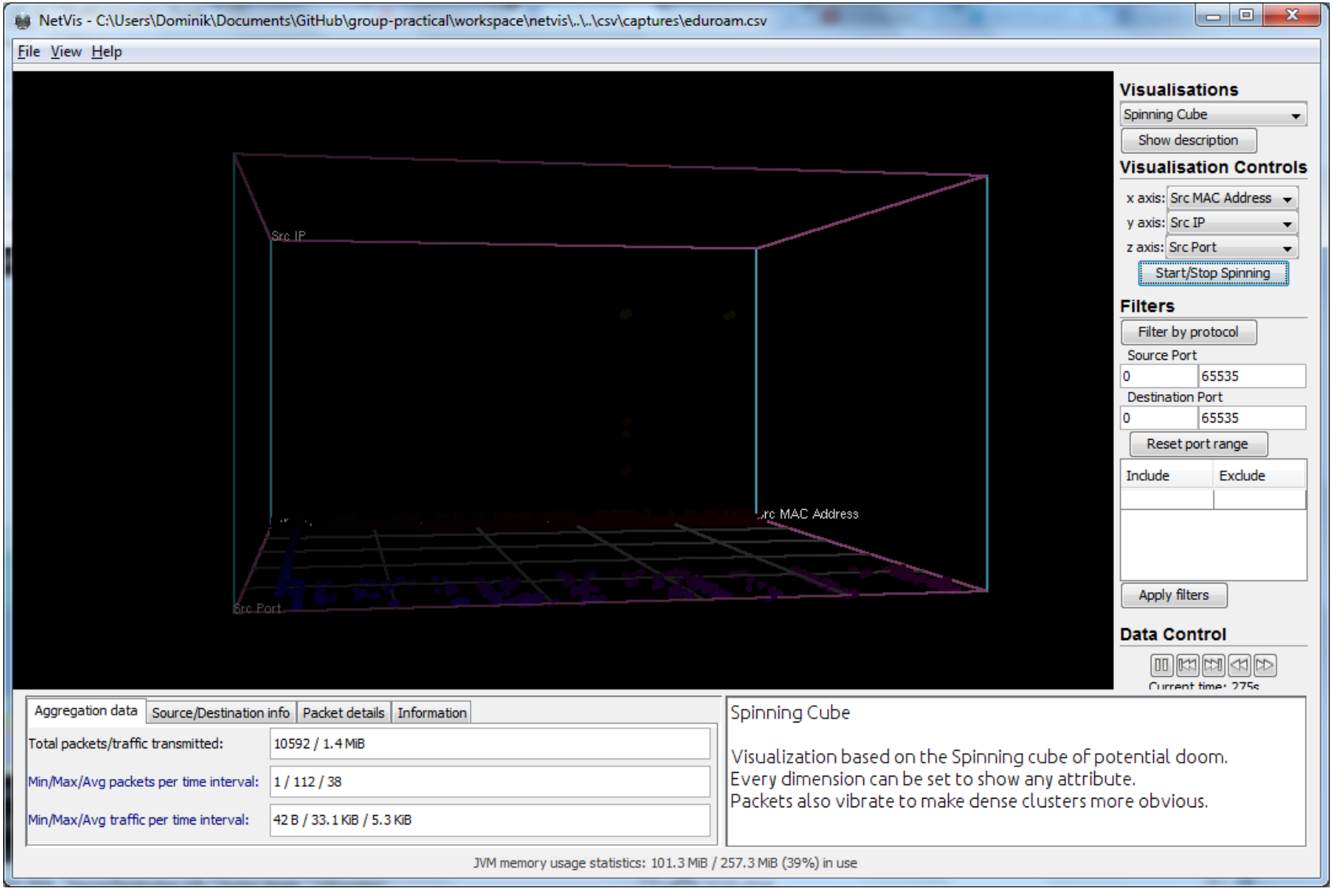
Dataflow Visualisation



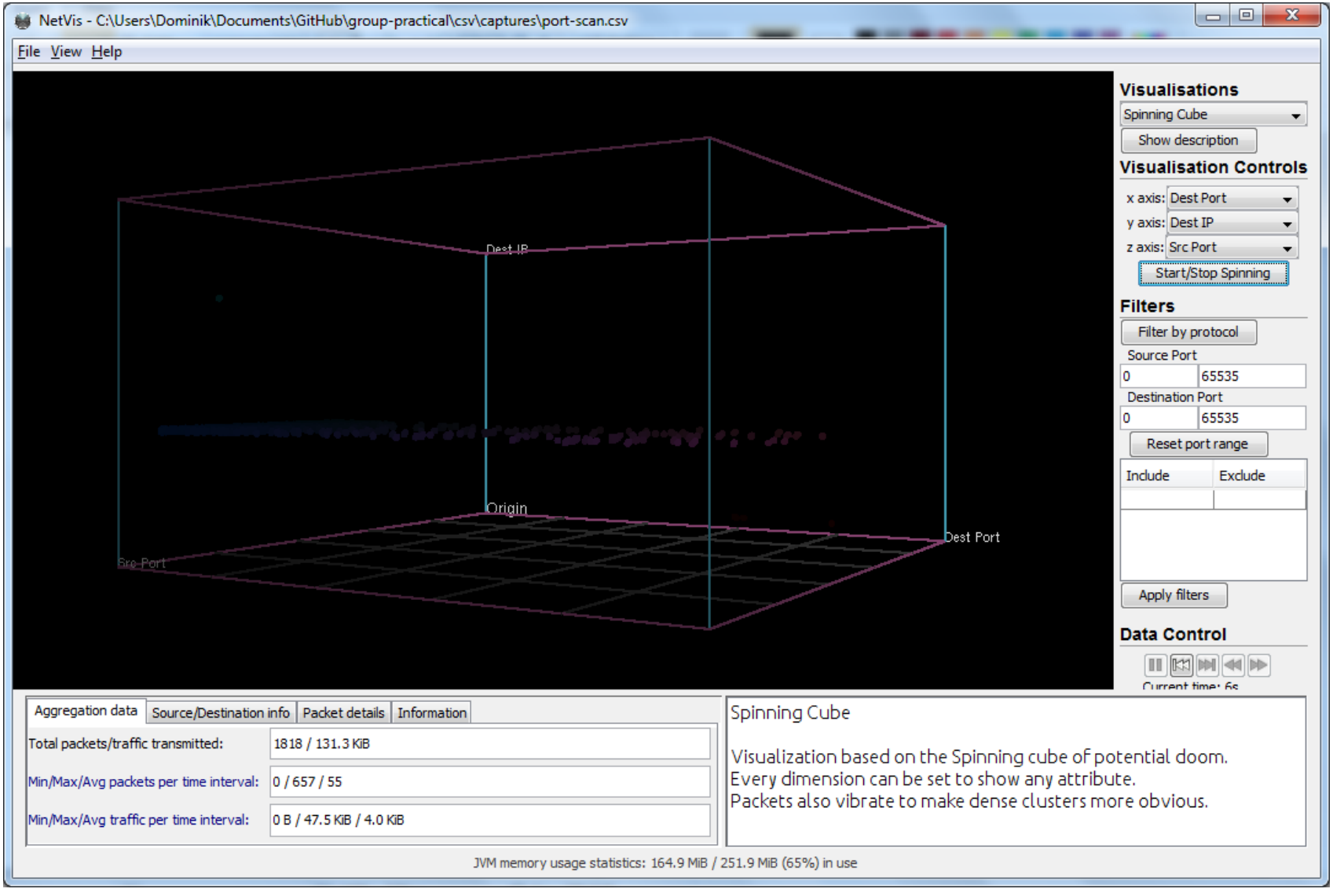
Port Scan Attack



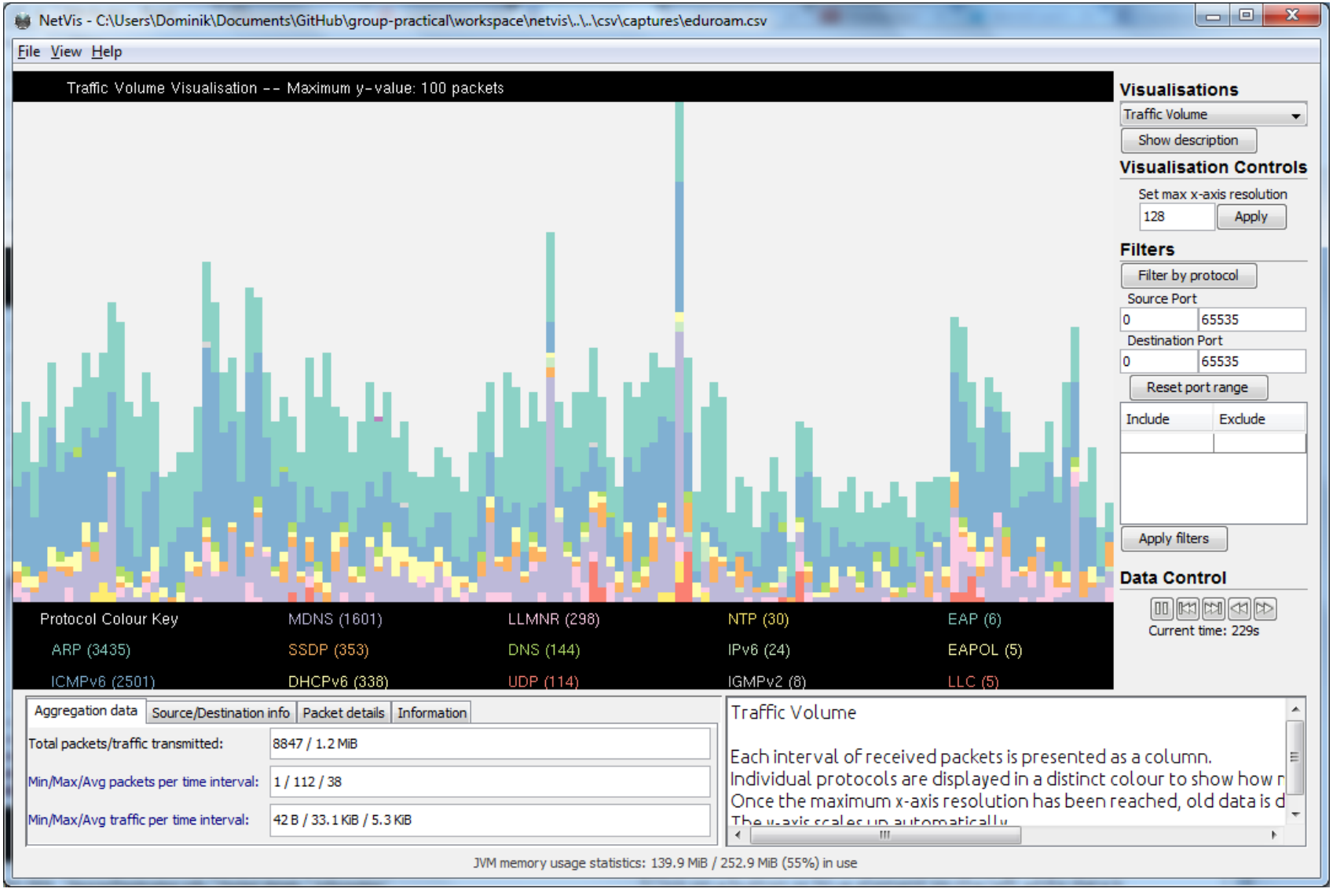
Spinning Cube Visualisation



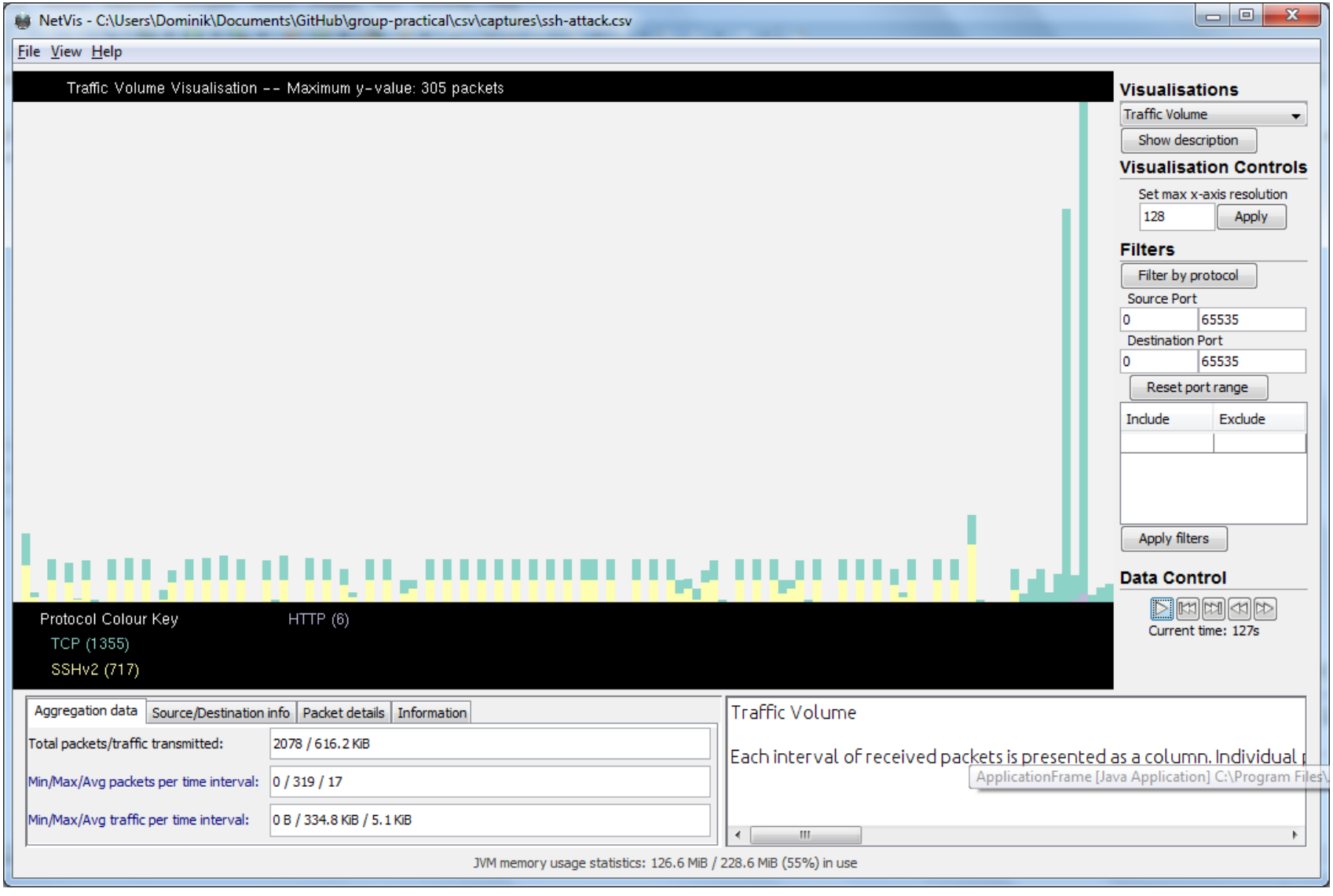
Port Scan Attack



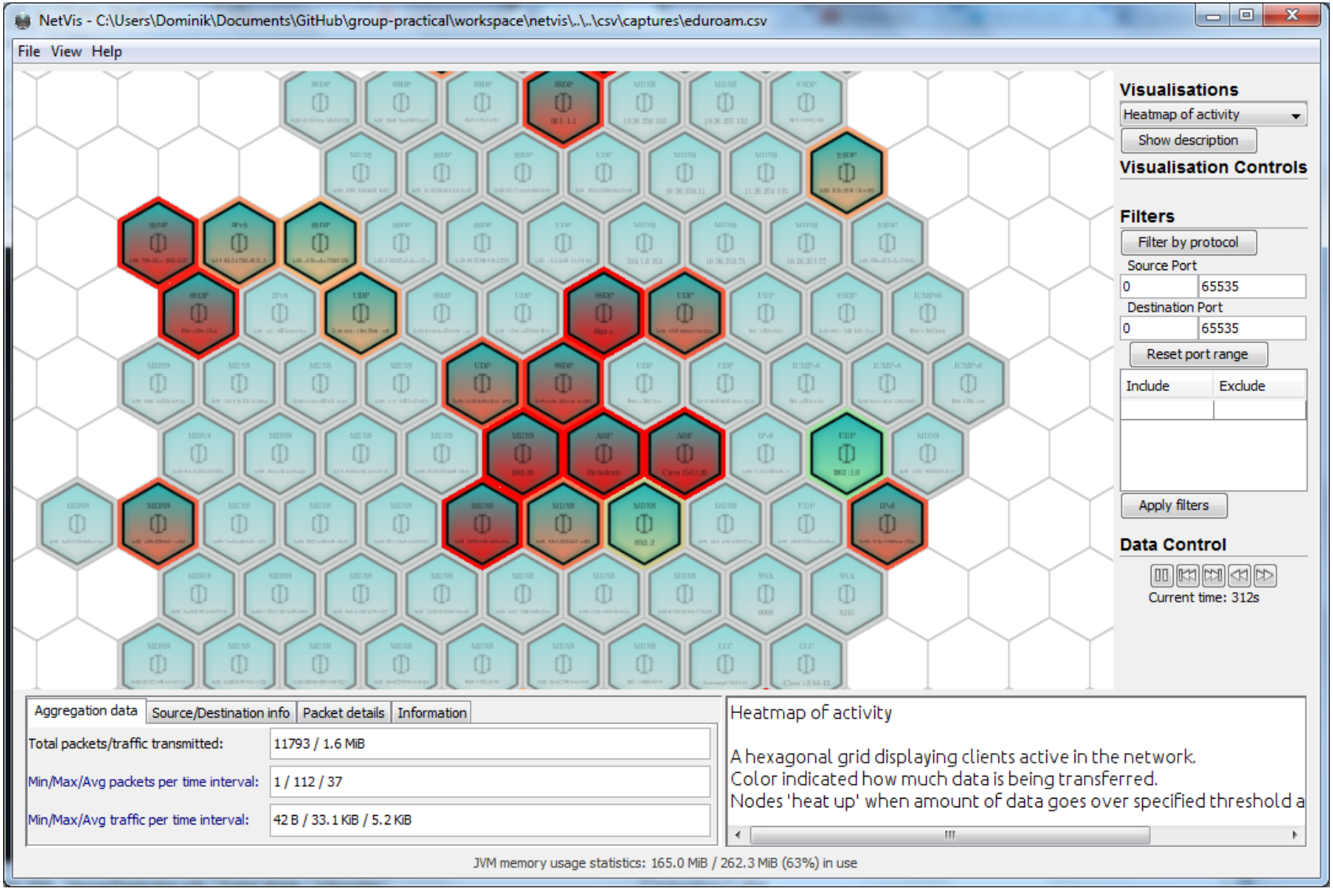
Traffic Volume Visualisation



SSH Brute Force Attack



Heat Map Visualisation



Activity Groups Visualisation