

The Honeyynet

P R O J E C T

Improving Picviz to dynamic and
visual log data analysis

Google summer of code

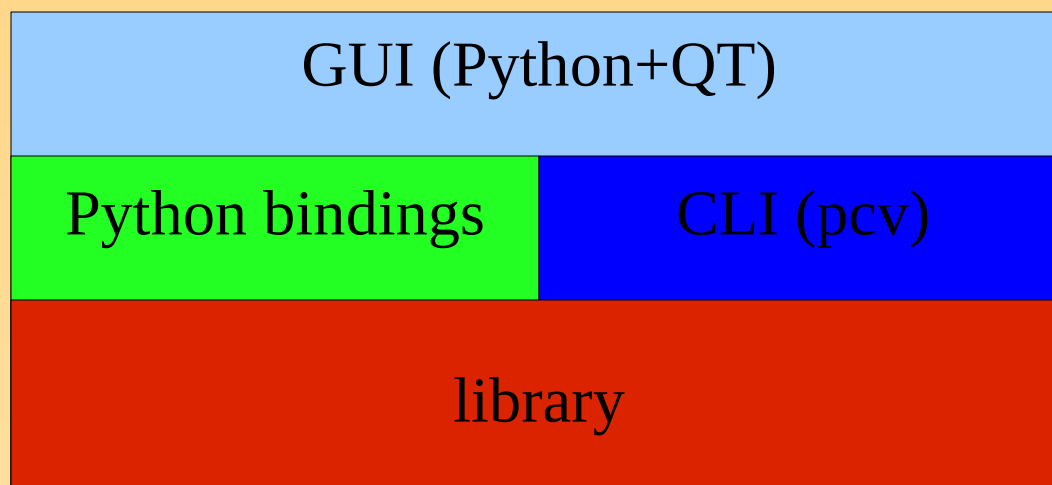
Mid-term status

Who?

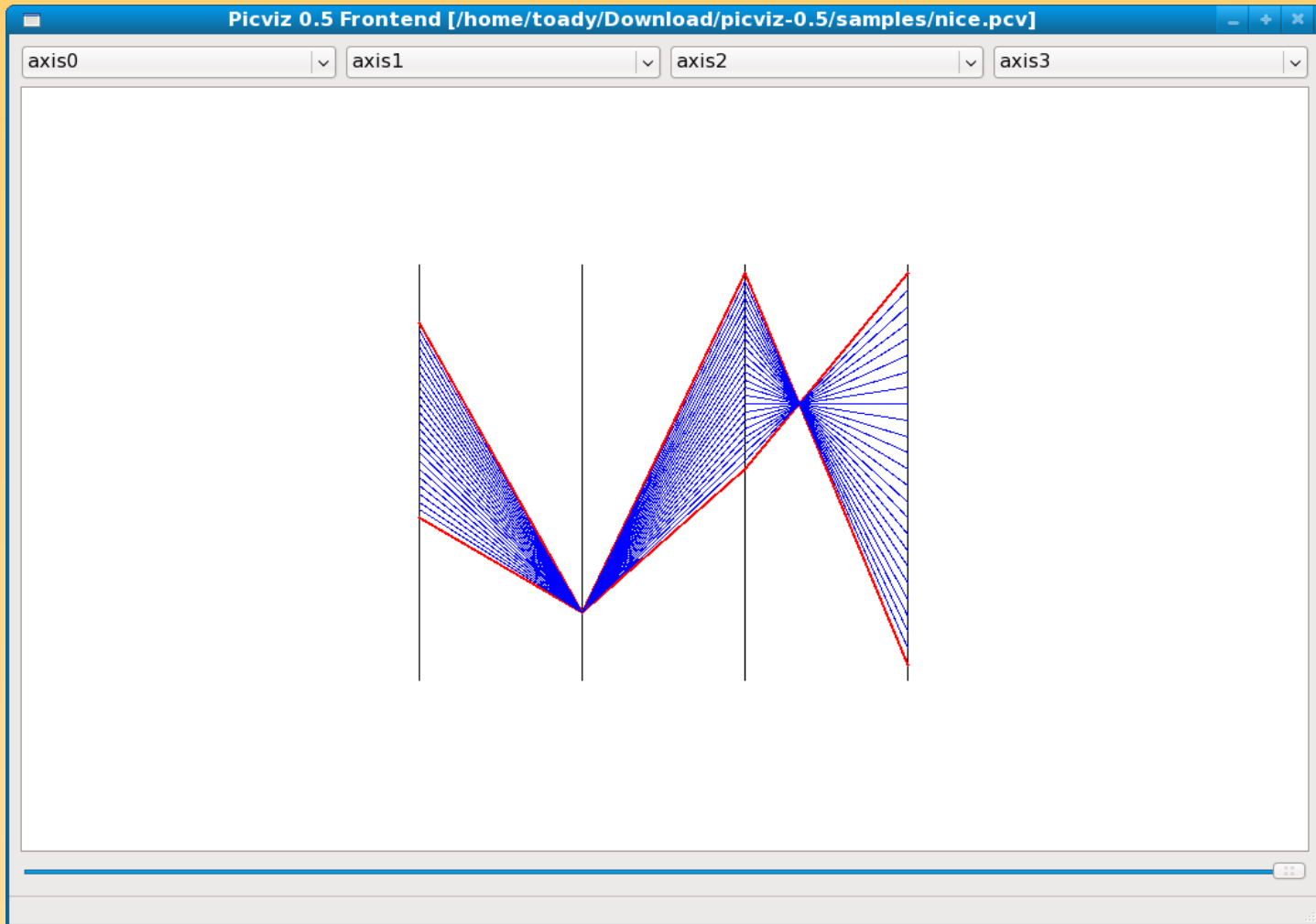
- Mentor: Sebastien Tricaud, French honeynet chapter lead
- Student: Victor Amaducci
- Contributor: Gabriel Cavalcante

What is Picviz?

- Generic parallel coordinates plot creator
- Focus on security



GUI status before GSOC



What we **could** (only) do

- See the axes name
- See the value on a given line
- Use the slider to navigate in the events timeline
- That was it... only those three things were featured

Our alien was sad...



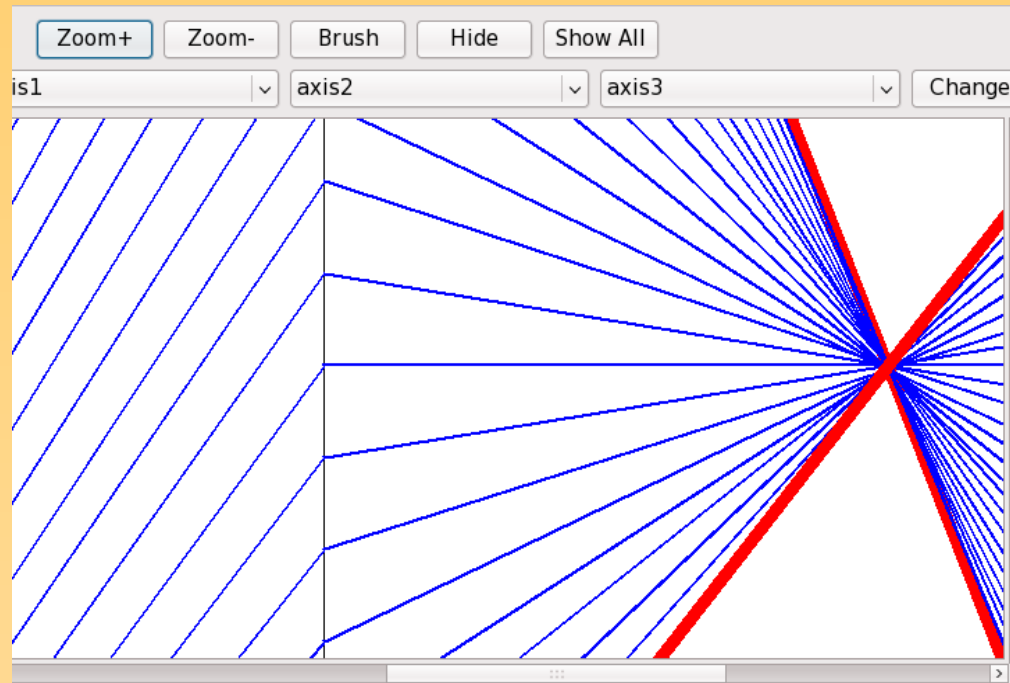
- Cannot reorder the axes on the fly
- No zoom
- No selection
- No possibility to see the full even
- No brushing...

Feature #1: Axes reordering



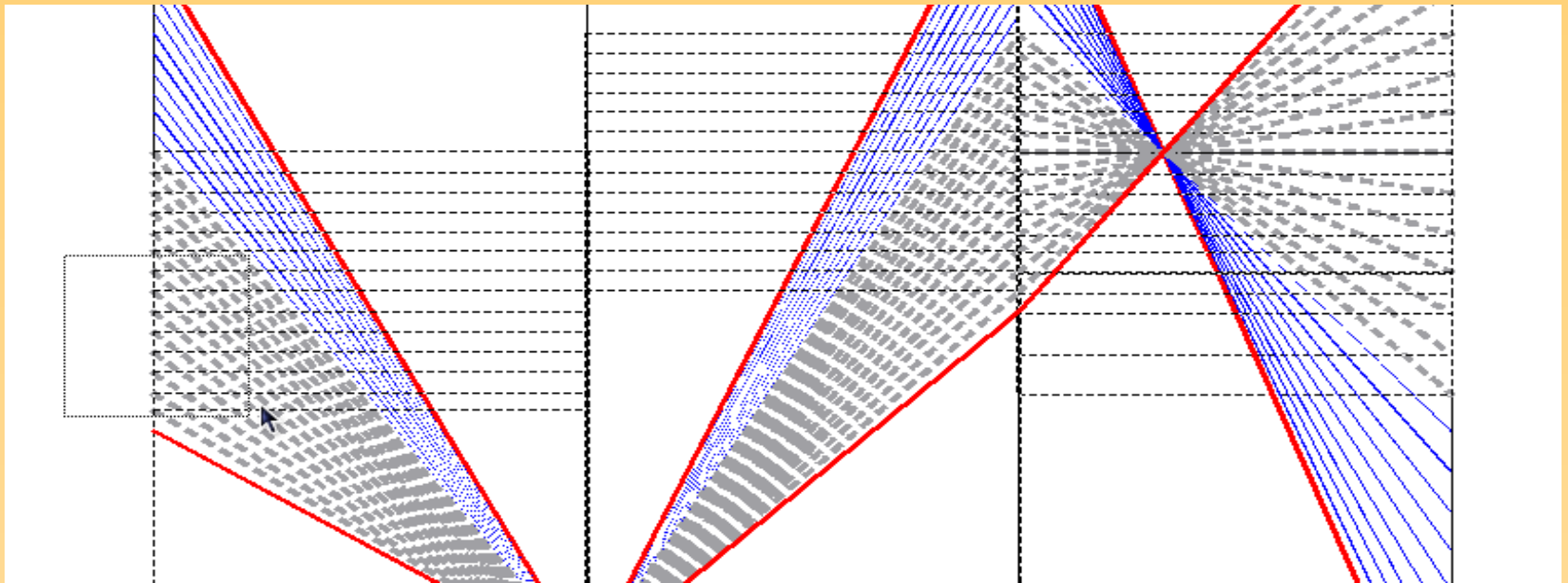
- Select the axis you want
- Click on Change

Feature #2: Zoom

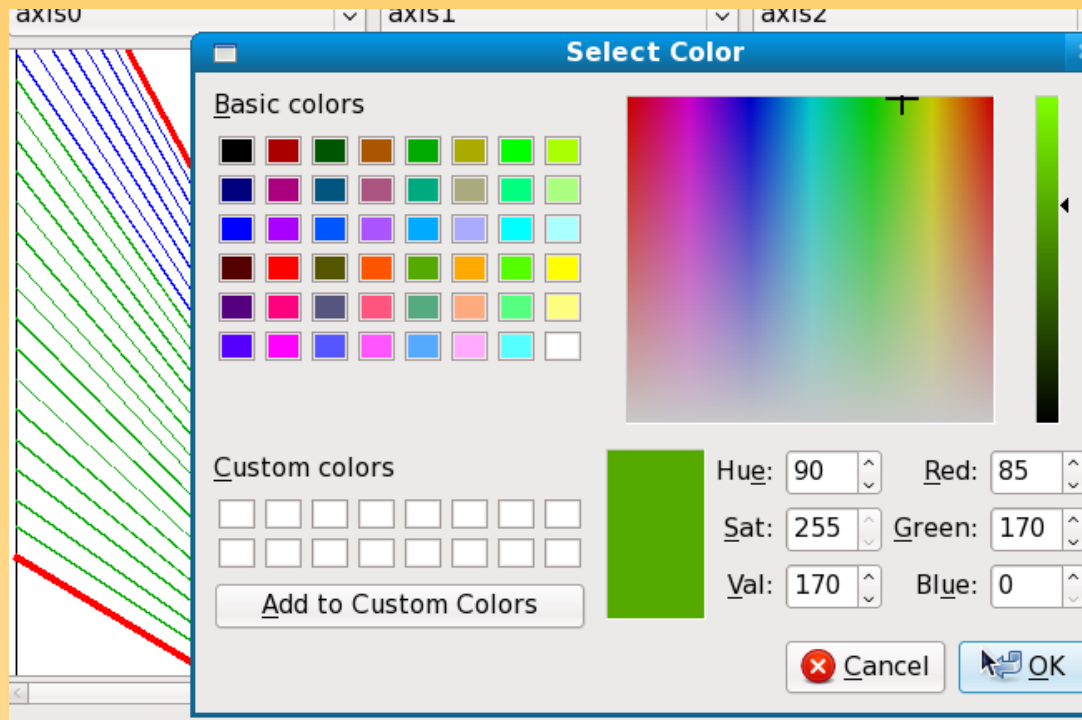


- Click on “Zoom+” or “Zoom-”

Feature #3: Selection

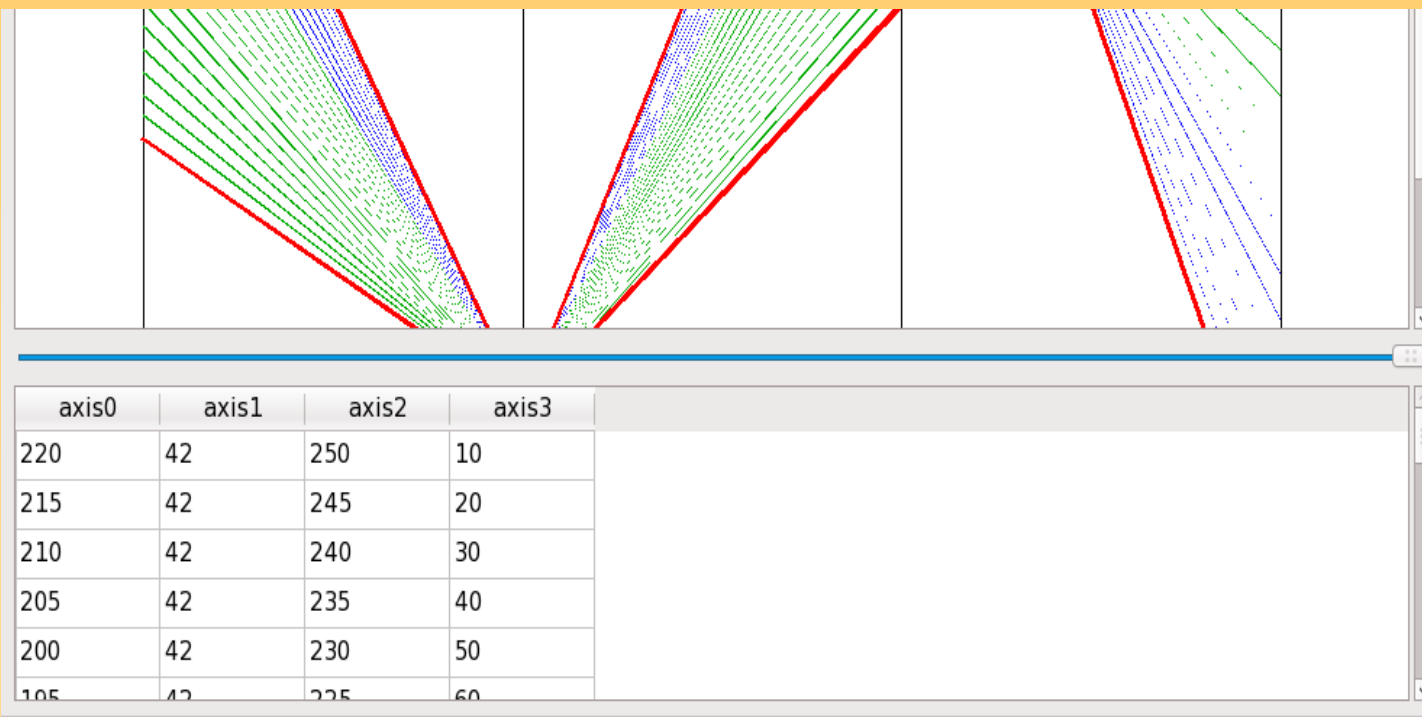


Feature #4: Brushing



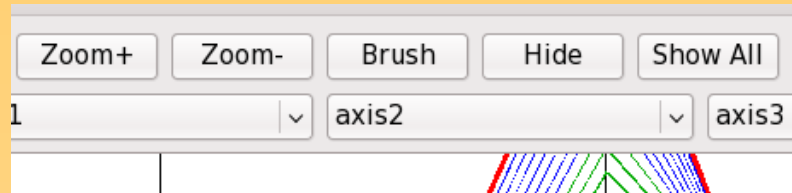
- Select lines
- Click on Brush and choose the color

Feature #5: See the full event



- The table below the graph displays the events: selecting a line will select the event.

Feature #6: Hide the unwanted



- Clicking on the 'Hide' button will hide the lines selected
- That will clear your graph
- You can show all lines hidden clicking on 'Show all' button

Thanks to the Google summer of code, our alien is happy now!



- This is only mid-term!
- Must-have features already in!

Future

- Ease the input from logs directly from the interface (syslog, network traffic...)
- Real-time (feature present in the library, used by the CLI, should be used by the GUI)
- Make the application faster
- ...