codilime®

CREATING VALUE

VELES: A new tool for binary file analysis

PWNing 2016

8/11/2016

What is VELES?

- A tool for analyzing binary code and data
- Statistical data visualizations
- Client-server model
- Open Source

Analysis

- PE, ELF, .class, PNG, ... file parsers
- Machine code and virtual machine bytecode disassemblers- (JVM,- Python,- Lua,- …)
- Decompiler to pseudocode (upcoming)
- User-directed analysis process (provide starting points, correct types, etc.)

Architecture

- Server stores parsed data information in database
- GUI is one of the clients (can be connected via network protocol)
- Ability to connect plugin-analyzers via same protocol

Visualizations

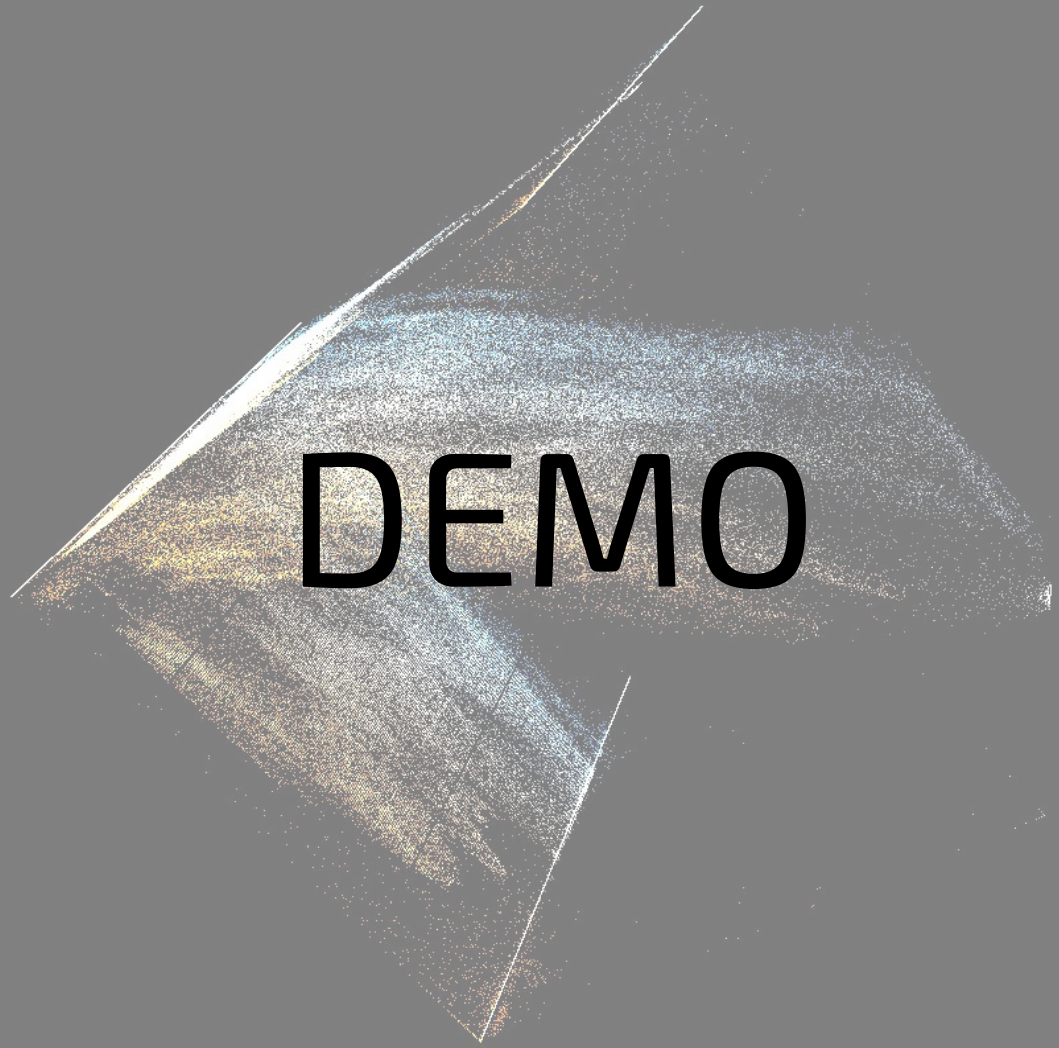
- Humans are good at noticing patterns in images
- Statistical visualization of any binary data
- Inspired by Christopher Domas' 2012 presentation (https://youtu.be/4bM3Gut1hIk) and the unreleased ..cantor.dust.. tool
- More info in the demo :)

Similar products

- IDA - excellent tool but expensive and not open-source
- Radare2 - no real GUI and bad overall UX, stability issues

Future

- Veles is now being used by CS16 - our CTF team
- Looking for other teams wanting to use Veles during CTF competitions
- Open-source release planned for January 2016
- Looking for community feedback


DEMO