GView

A Smart Generic Visualizer Assistant for Security Analysis

GView

A framework designed to provide **generic visualization** for various file types with **automatic identification** and **artifact extraction** and reanalysis.

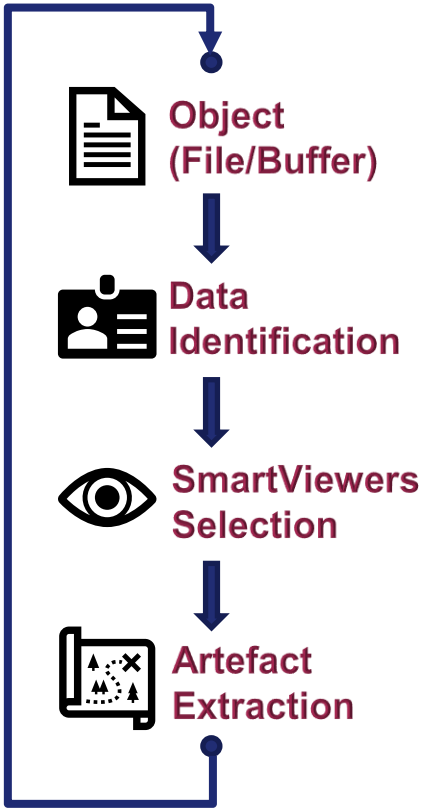
GView was designed with **3 major use-cases** in mind:

Forensics Investigations

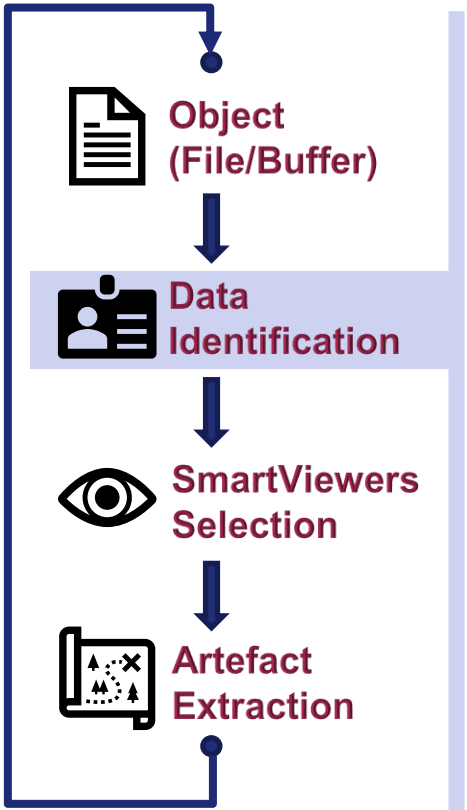
Security Operation Centers

Security vendors: In-lab plugins

GView architecture overview



GView architecture overview



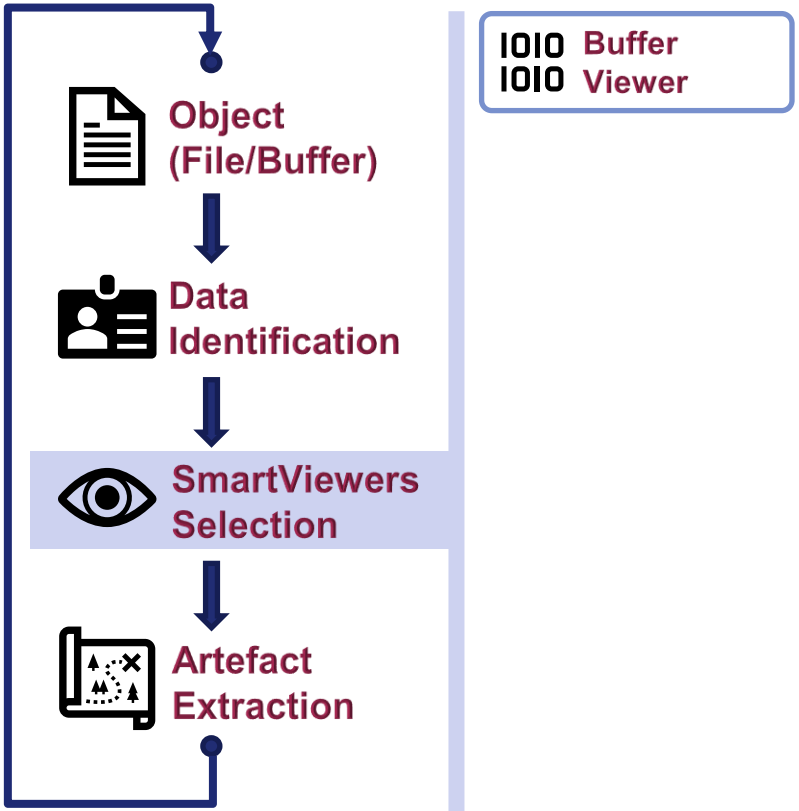
Binary Content

- **Network analyzers** (e.g. PCAP)
- **Images**(e.g. BMP, Icons, Cursors)
- **Binary files** (e.g. PE, ELF, Macho)
- **Archives** (e.g. ZIP, ISO)

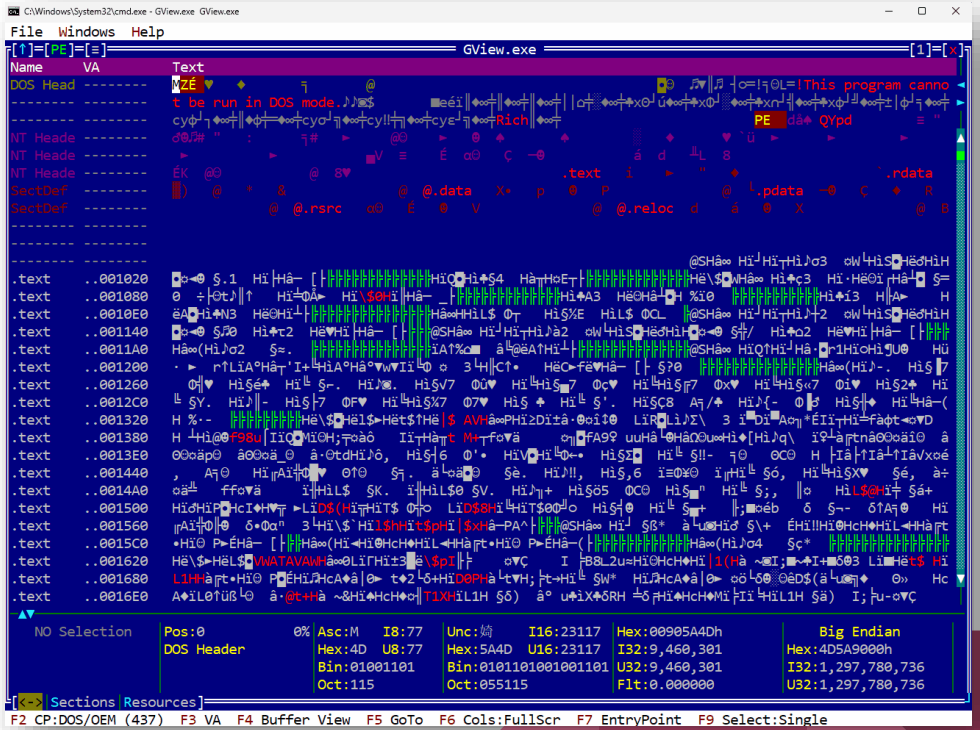
Text / readable Content

- **Scripts** (e.g. JavaScript, VBA)
- **Configuration files** (e.g. INI,TOML,JSON)
- **Data files** (e.g. CSV, TSV)
- **Programming languages** (e.g. C++)

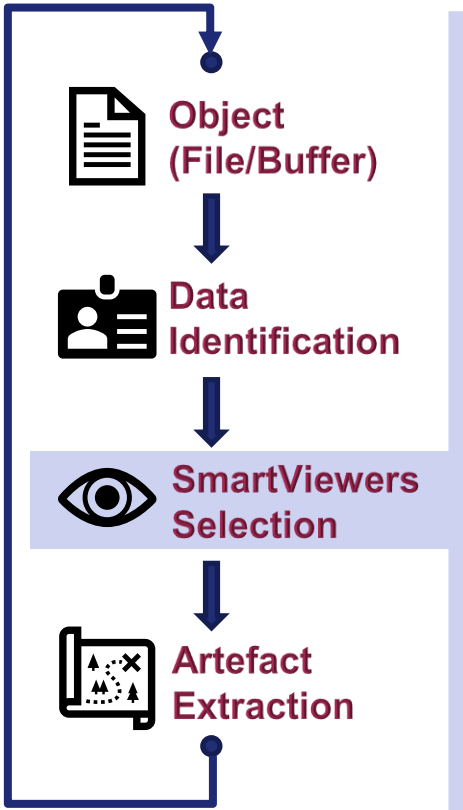
GView architecture overview



Buffer
Viewer

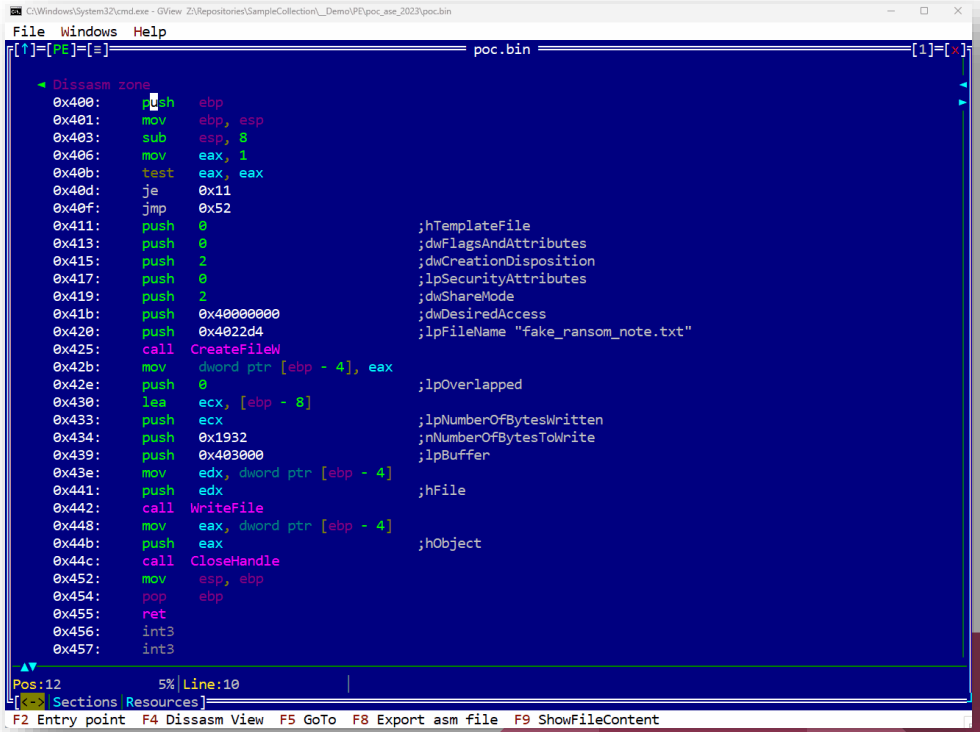


GView architecture overview

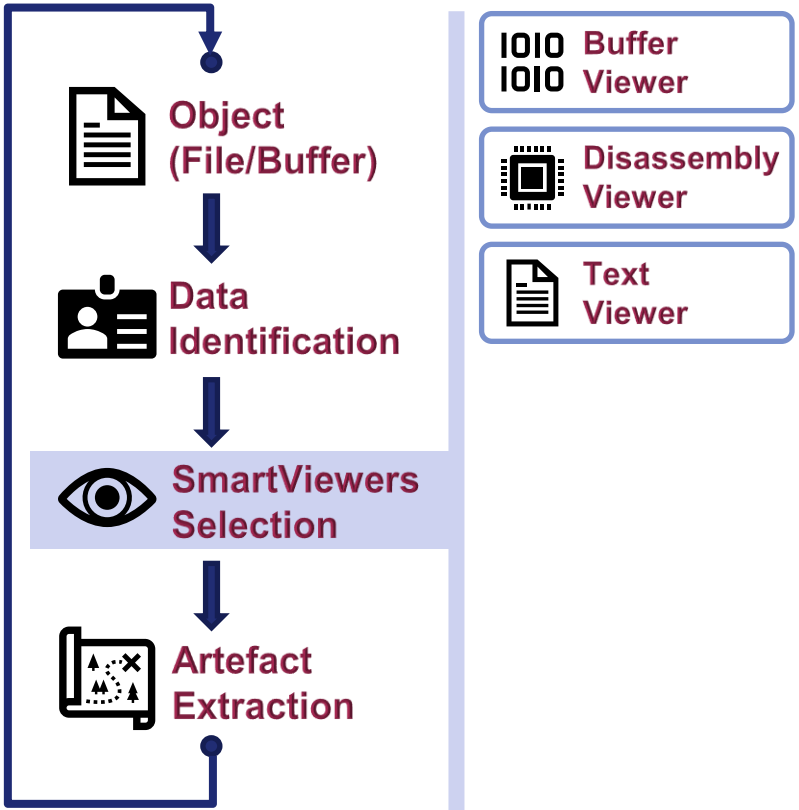


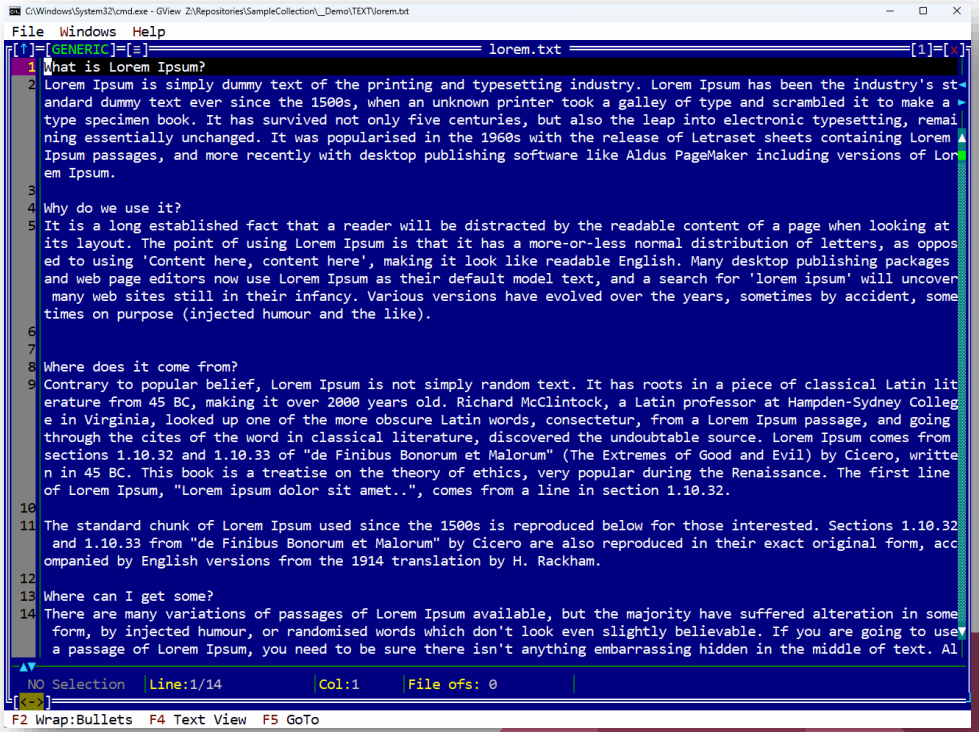
Buffer Viewer

Disassembly Viewer

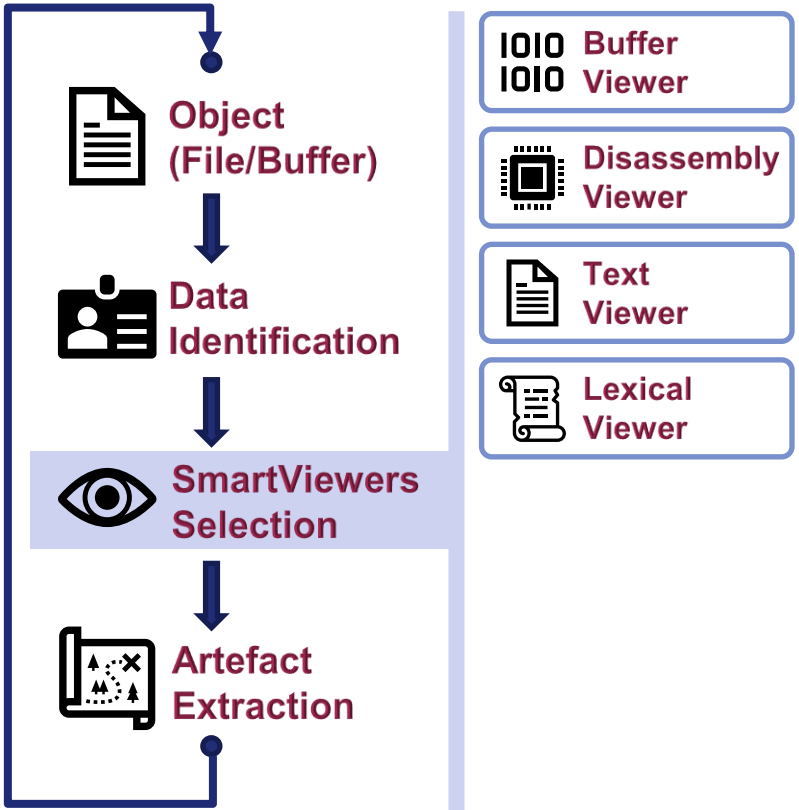


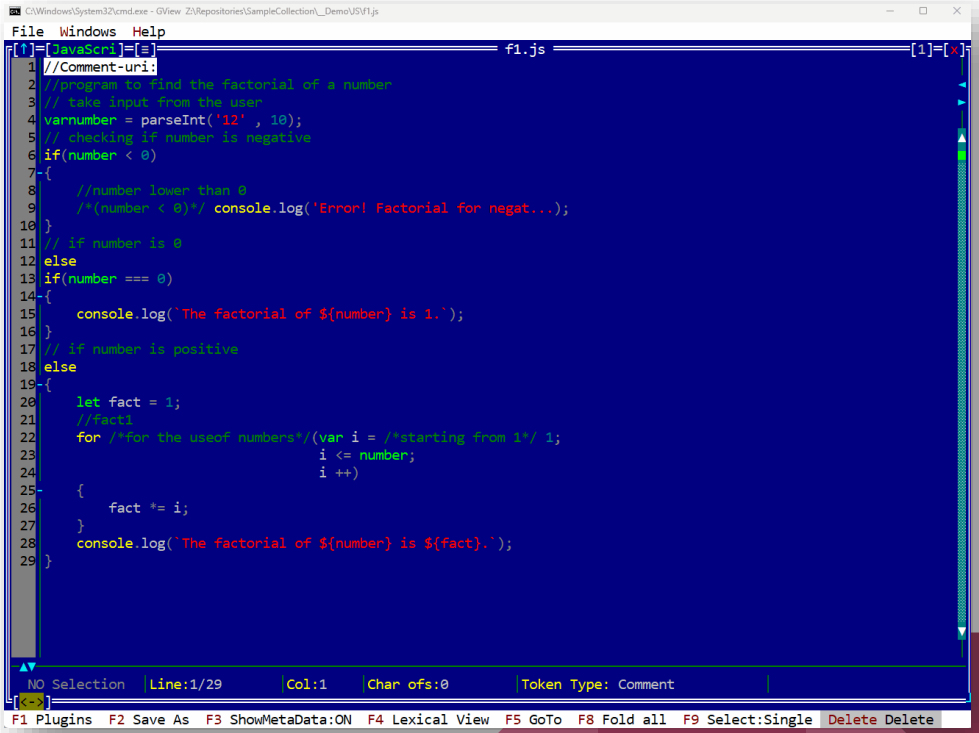
GView architecture overview



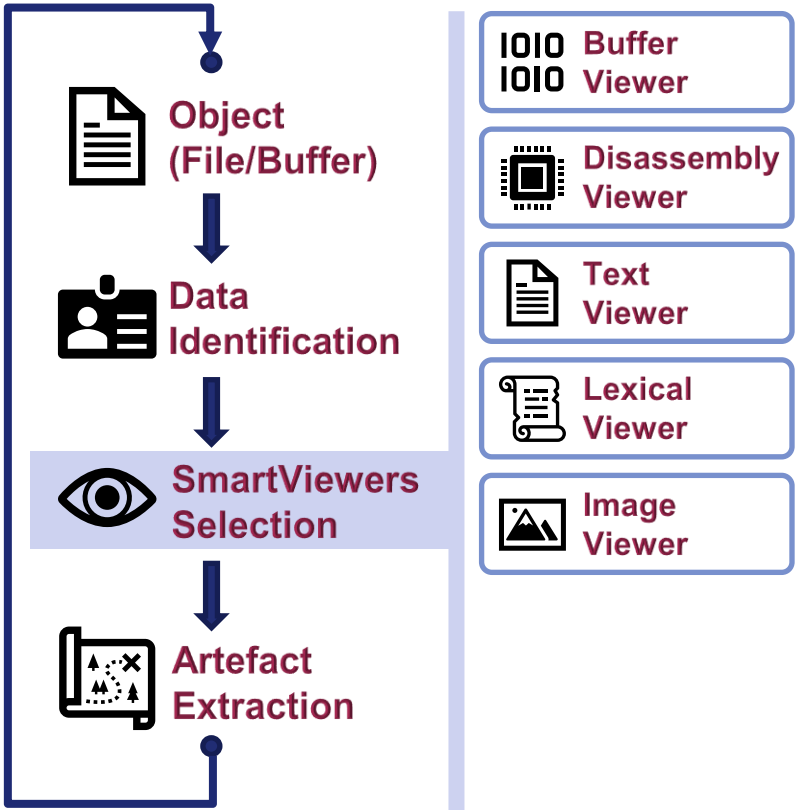


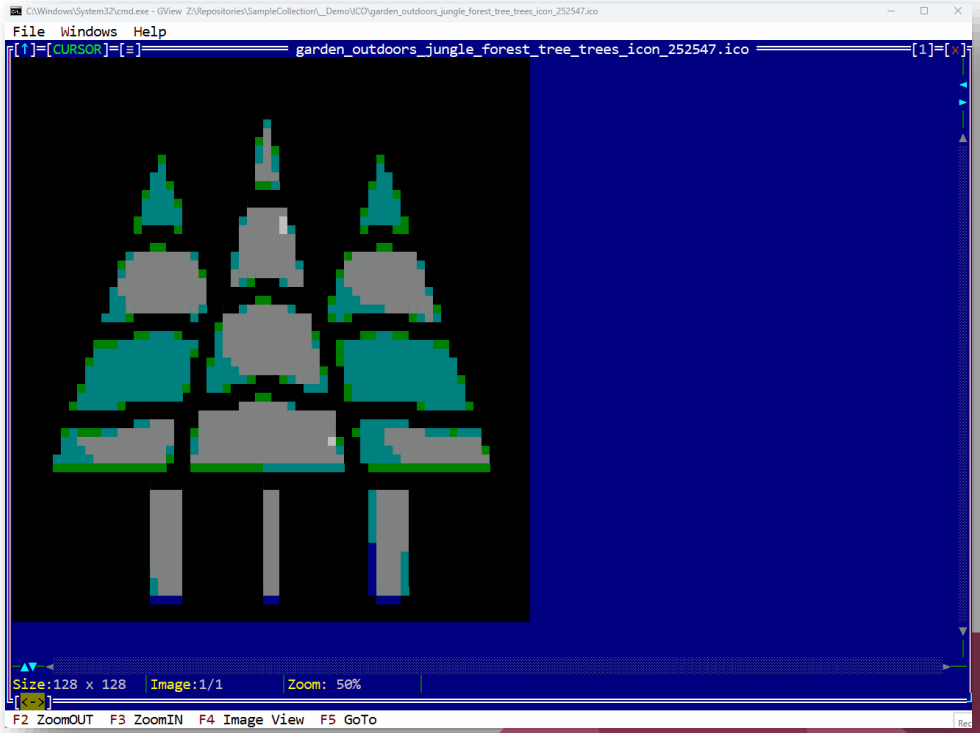
GView architecture overview



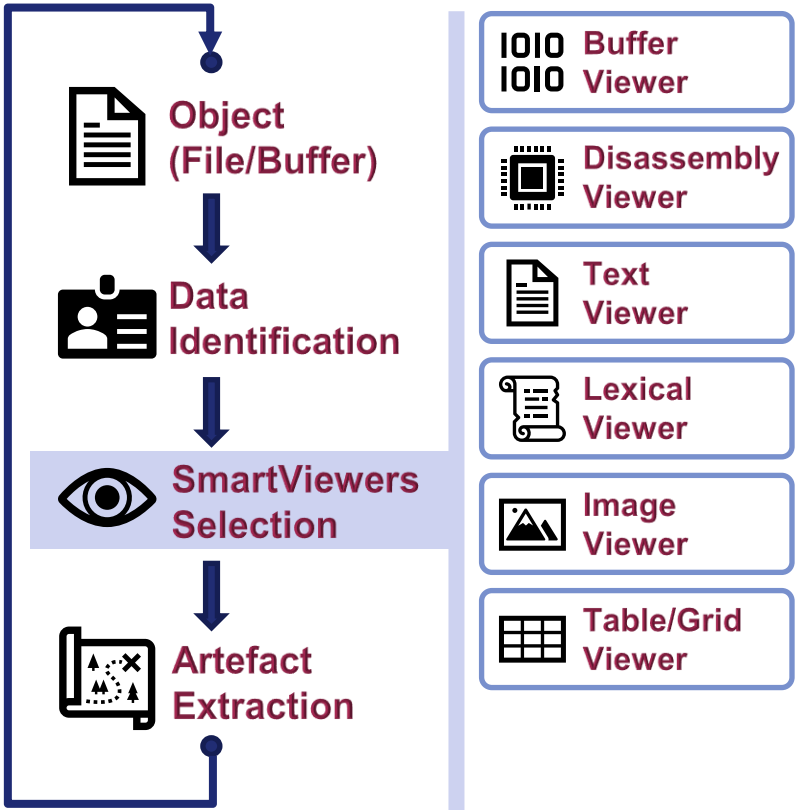


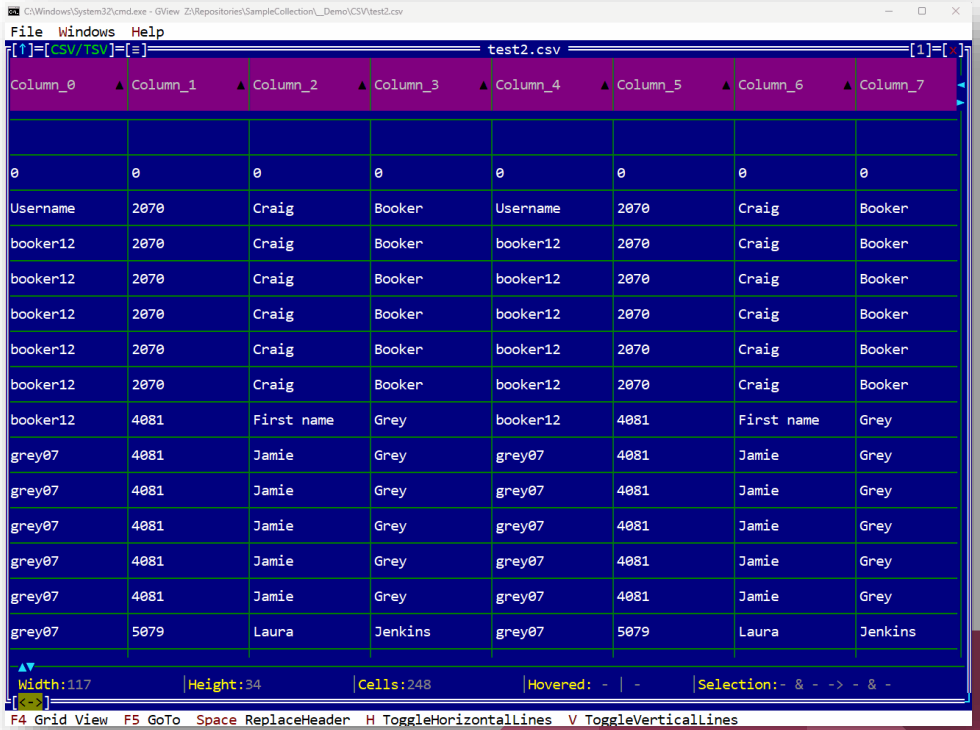
GView architecture overview



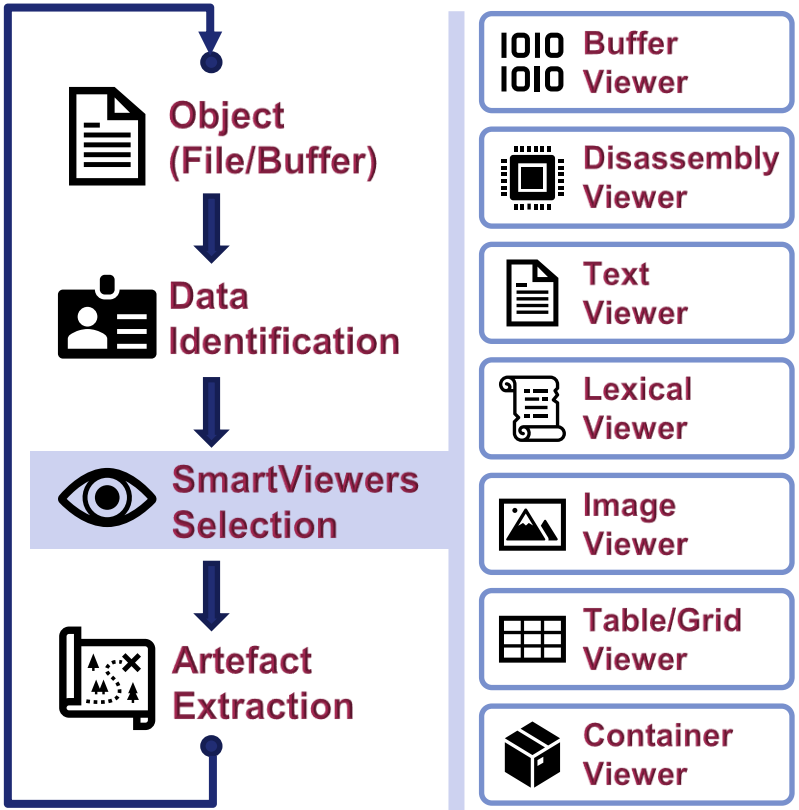


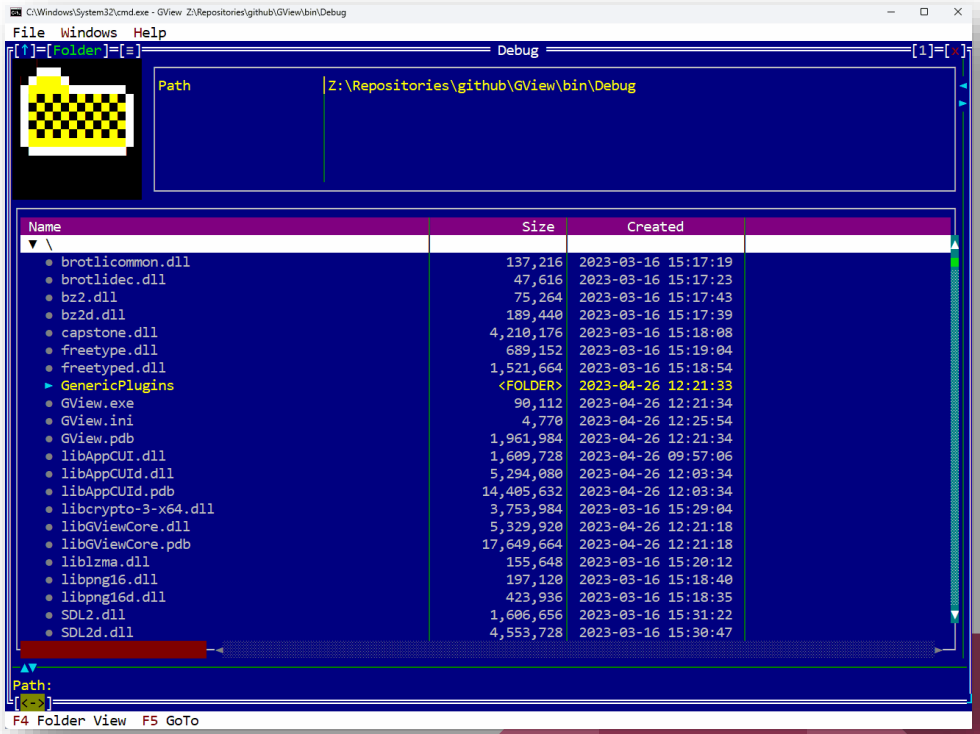
GView architecture overview





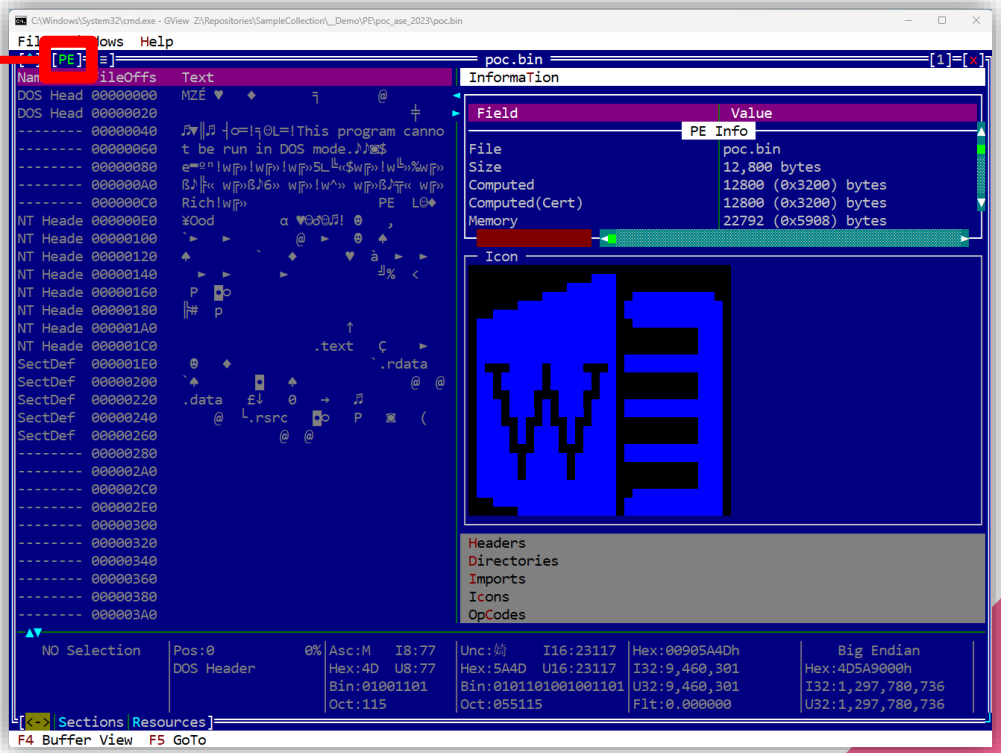
GView architecture overview



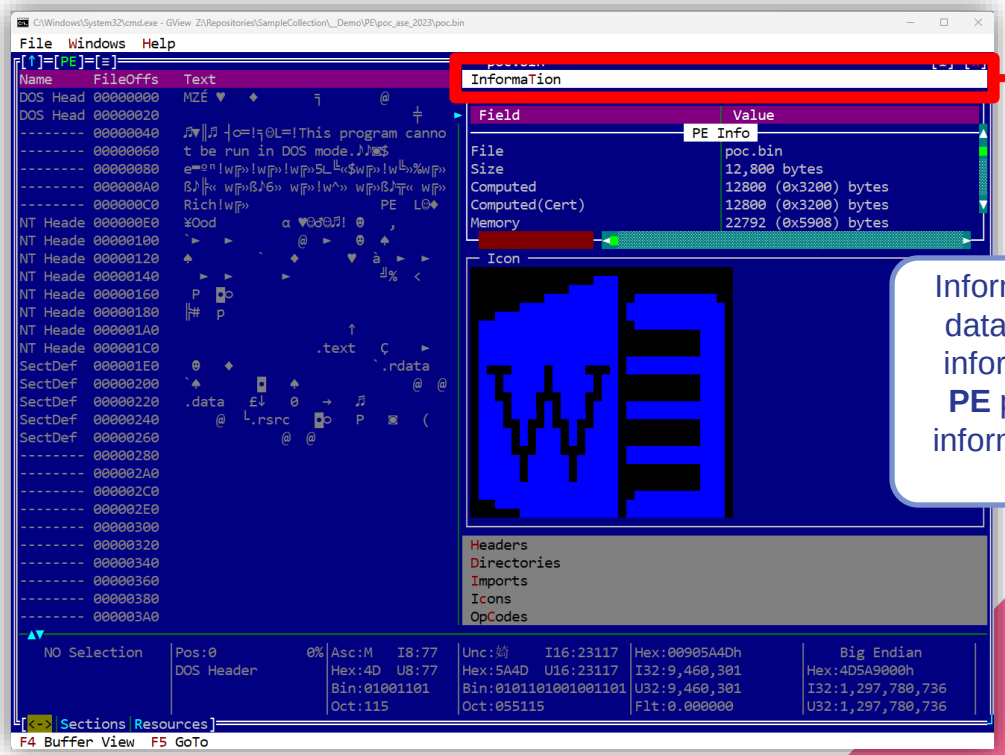


UX Overview

Data type plugin (in this case **PE**)



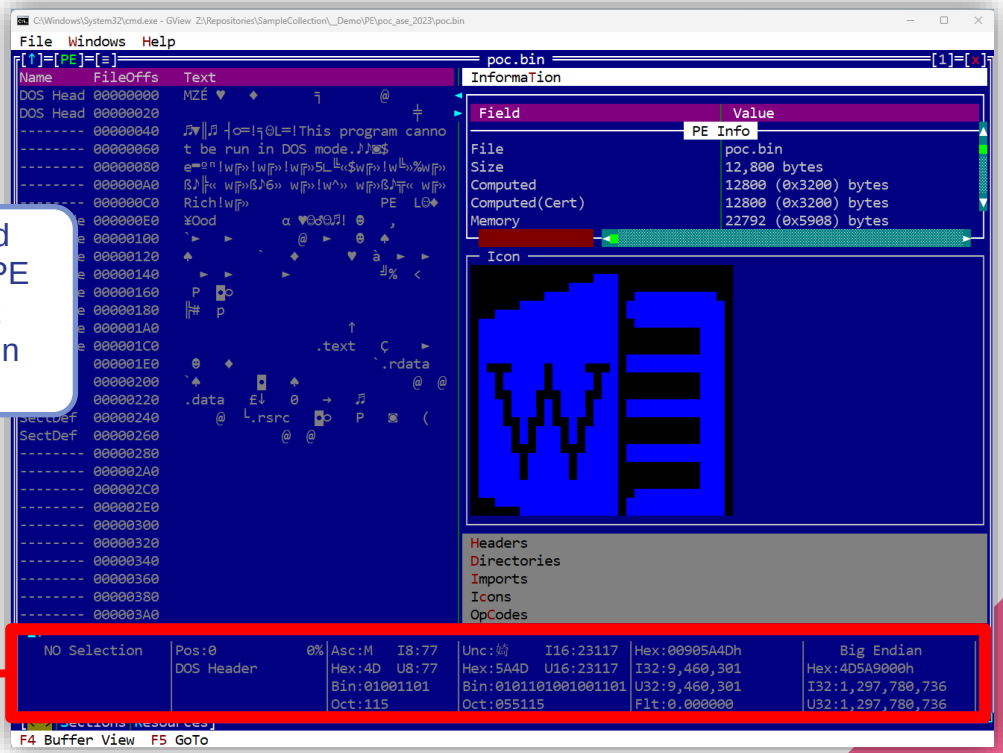
UX Overview



Information Panel (where each data type plugin adds various information). For example the **PE** plugin prints here version information, icon, export name, PDB path, …

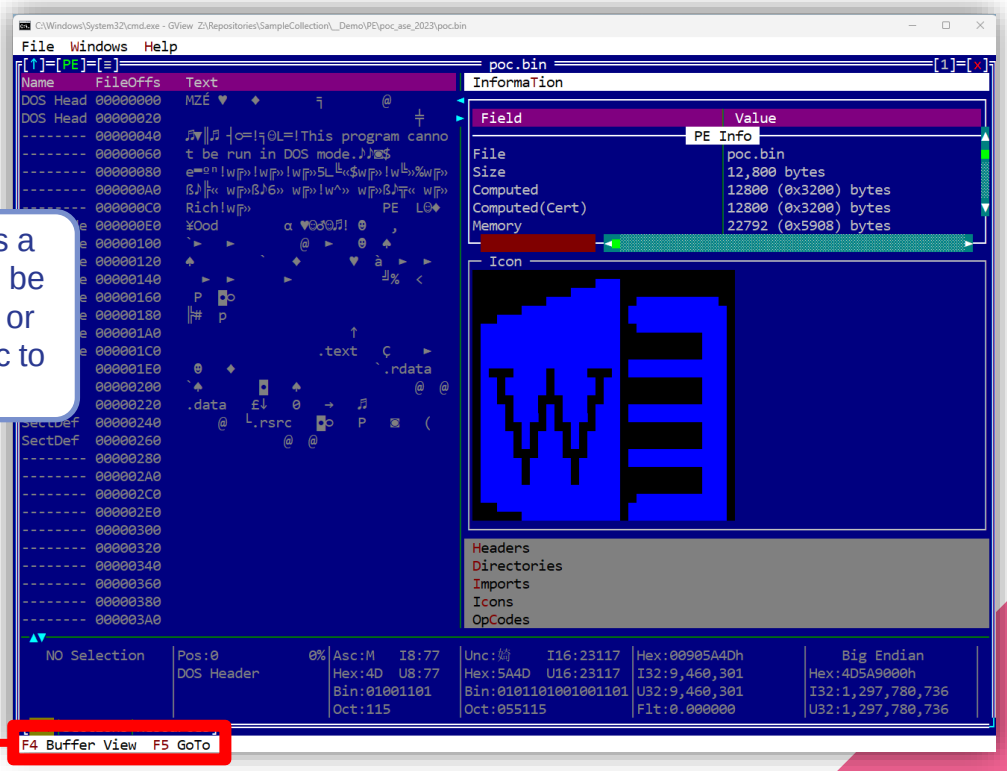
UX Overview

This area presents cursor and selection information. For the PE file it also computes different values (such as hex values, bin values, float values, etc)



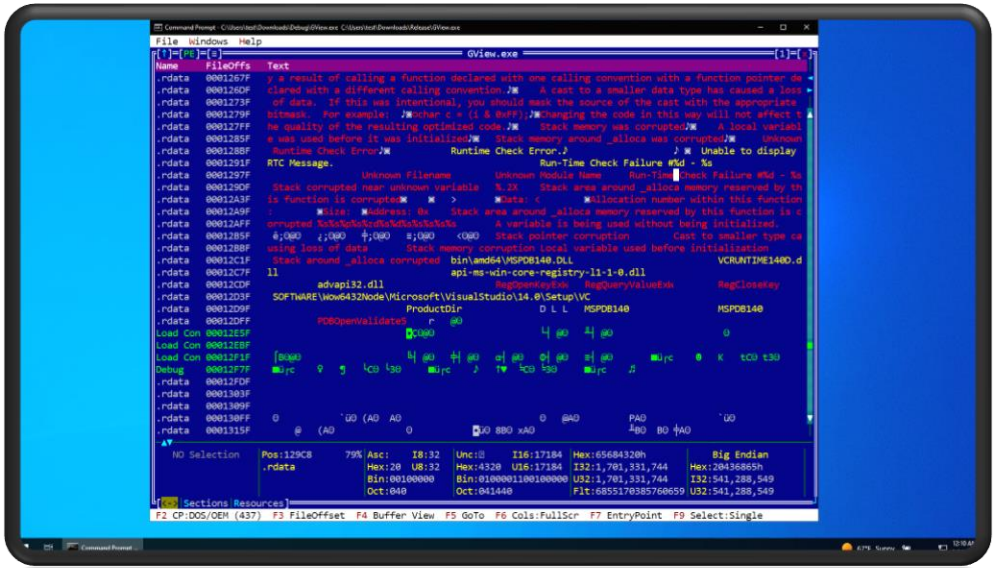
UX Overview

Finally, the bottom bar contains a list of quick commands that can be used to either change the view or to perform various tasks specific to the view or data plugin.



Suported OS architecture

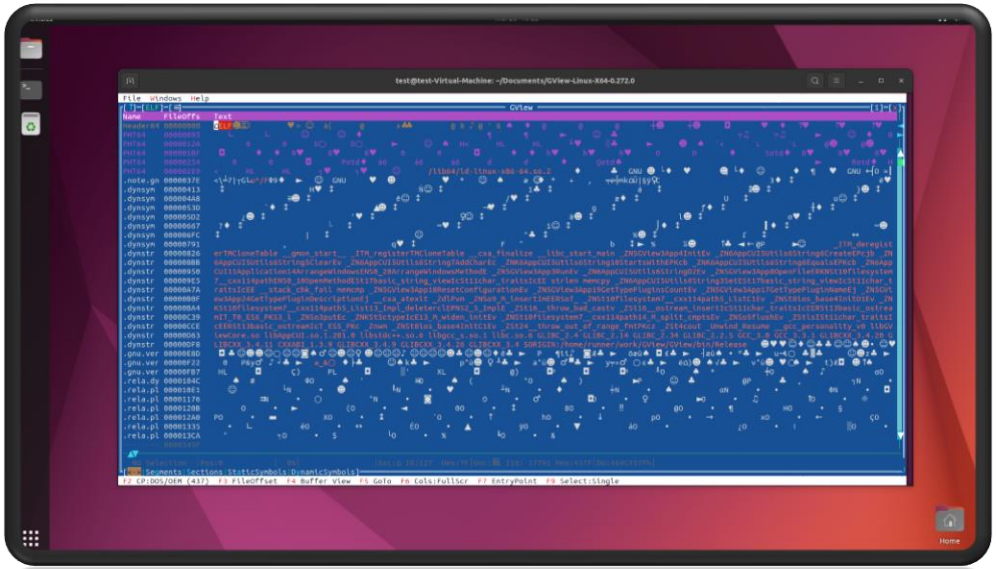
Microsoft Windows



Suported OS architecture

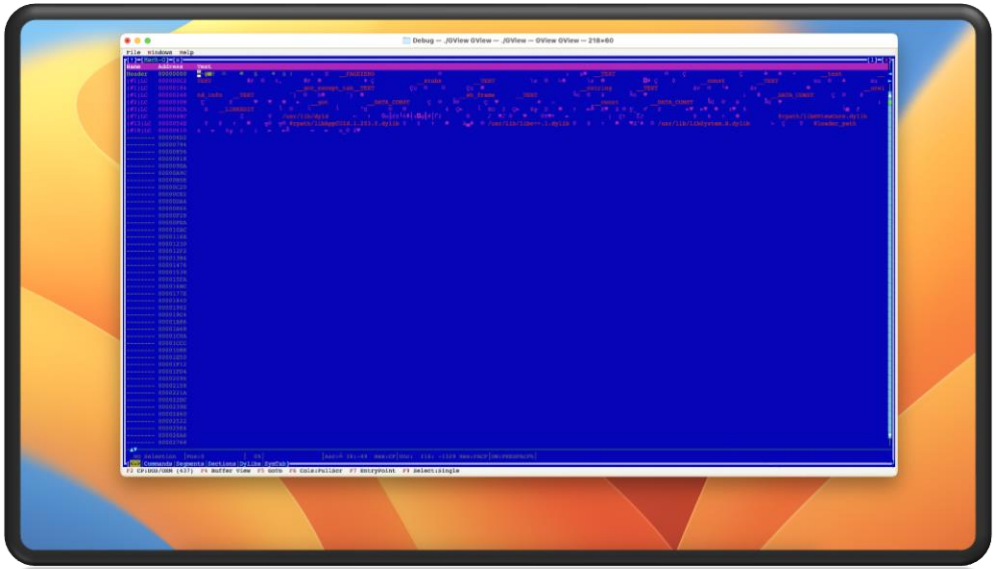
Microsoft Windows

Linux (ex. Ubuntu)



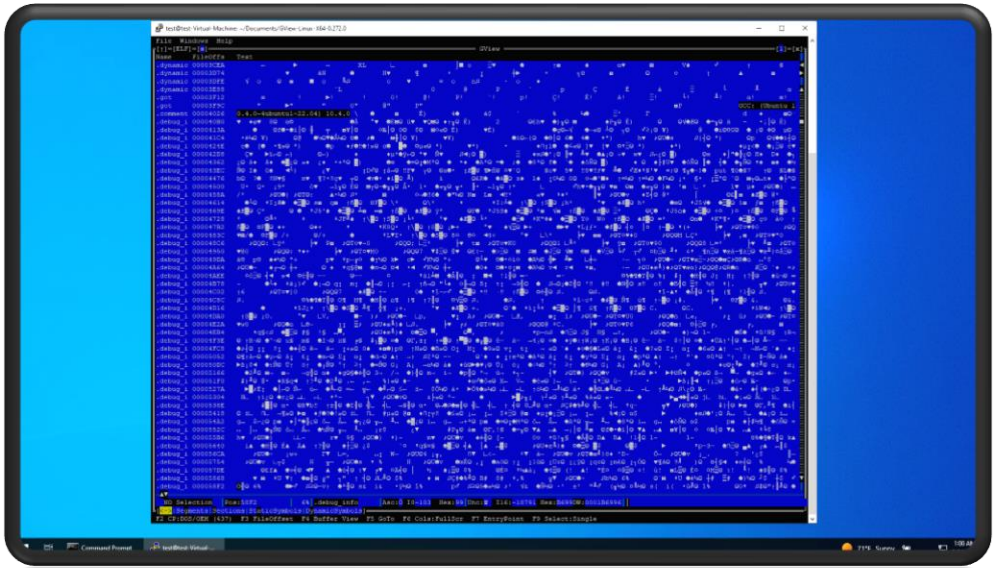
Suported OS architecture

- Microsoft Windows
- Linux (ex. Ubuntu)
- Apple MacOS



Suported OS architecture

- Microsoft Windows
- Linux (ex. Ubuntu)
- Apple MacOS
- Remote via SSH connections



Demo

For the demo purposes we have build a POC traffic capture that resembles a ransomware attack. No actual malware or any piece of malicious code were used in this demo.

Conclusions & Future Work

Conclusions

- Security framework for Forensic Engineers and Malware researchers
- Cross platform compatibility
- Security Operation Center assess solution

Future Development

- Email support
- Office files (Macro VBA extractor)
- PowerShell parser and deobfuscator
- Support for in-memory analysis

Thank you !