# WHEN WORLDS COLLIDE

r4ghidra

# WHOAMI

- buherator
  - Hungary (title background by Conspiracy)
- Security Researcher @ PixiePoint Security
- Ghidra nerd
  - No affiliation with NSA :)
- Weird targets, weird bugs, weird solutions

# AGENDA

- r4ghidra
- High dose of dev content, sry!
  - We need better tools
  - We need **integration**
- Request for feedback
  - There will be surveys
  - Links/QR's will be shown at the end too
- A surprise for the RE crowd
  - Stay tuned

# MOTIVATION

*"I don't use $tool but I buy the license every year just so that IDA has competition" - [REDACTED]*

# ORIGINS

# GHIDRA-R2WEB

Ghidra integration for r2

- By pancake
- From 2019
- Last commit in 2021 before I picked up in 2024
- Java script for Ghidra (not JS!)
- Communication via r2web protocol

# R2WEB IS GREAT

*"This is HTTP, I know this!"*

- Great tooling and language support
- High flexibility
- Human *and* machine readable
- Easy to debug

# GHIDRA-R2WEB INTEGRATIONS

## Pain points

- Single-file Java code
- Event handling @ Ghidra side (server stop/restart)
- Debugging

# FIRST REWRITE

- Ghidra extension (+ headless support)
- IDEA integration
- Small set of commands
- Improved HTTP handling
- OO command parser

It works!

# R2WEB DEMO

# USE-CASES

## ghidra-r2web

- Utilize Ghidra's loaders and analyzers
  - r2web can supply raw bytes for r2
- Sleigh
  - Disassembler
  - Decompiler

# PROJECTS NEED COMMUNITY FEEDBACK!

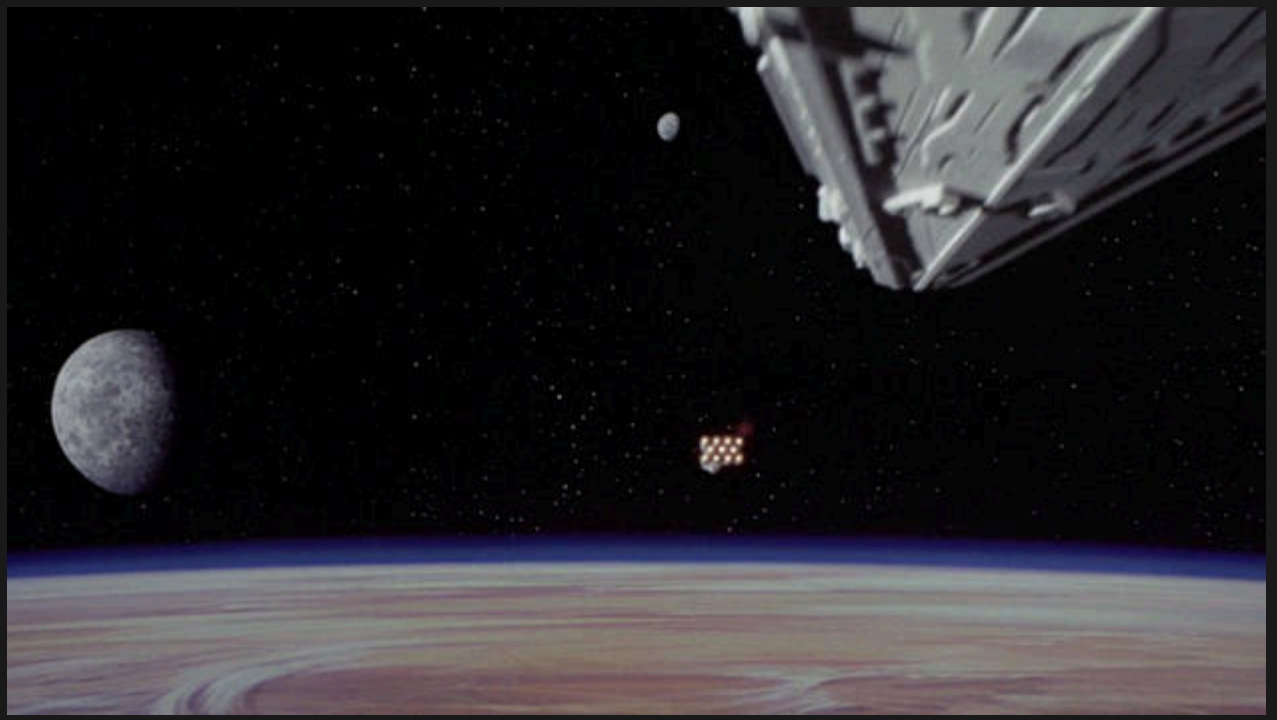
- *Lots* of development to do
  - We *must* prioritize!
- Motivation
- Half of the integrators aren't familiar with the workflow of the other half

# R4GHIDRA-R2WEB FEEDBACK FORM

# WEAK POINTS

- Adding commands was slow
  - r2 skill issue, sry
- States are not synchronized
  - Design property

# A NEW REPL



# A NEW REPL

- Pancake to the rescue!
- "28 files changed / +6083 -1 lines changed"
  - ~500% LoC increase
- No tests

# WHEN THE DUST SETTLED

- We have a REPL *in Ghidra*
- Fully transpiled r2 command handling
- Lots of features implemented

# R4GHIDRA REPL DEMO

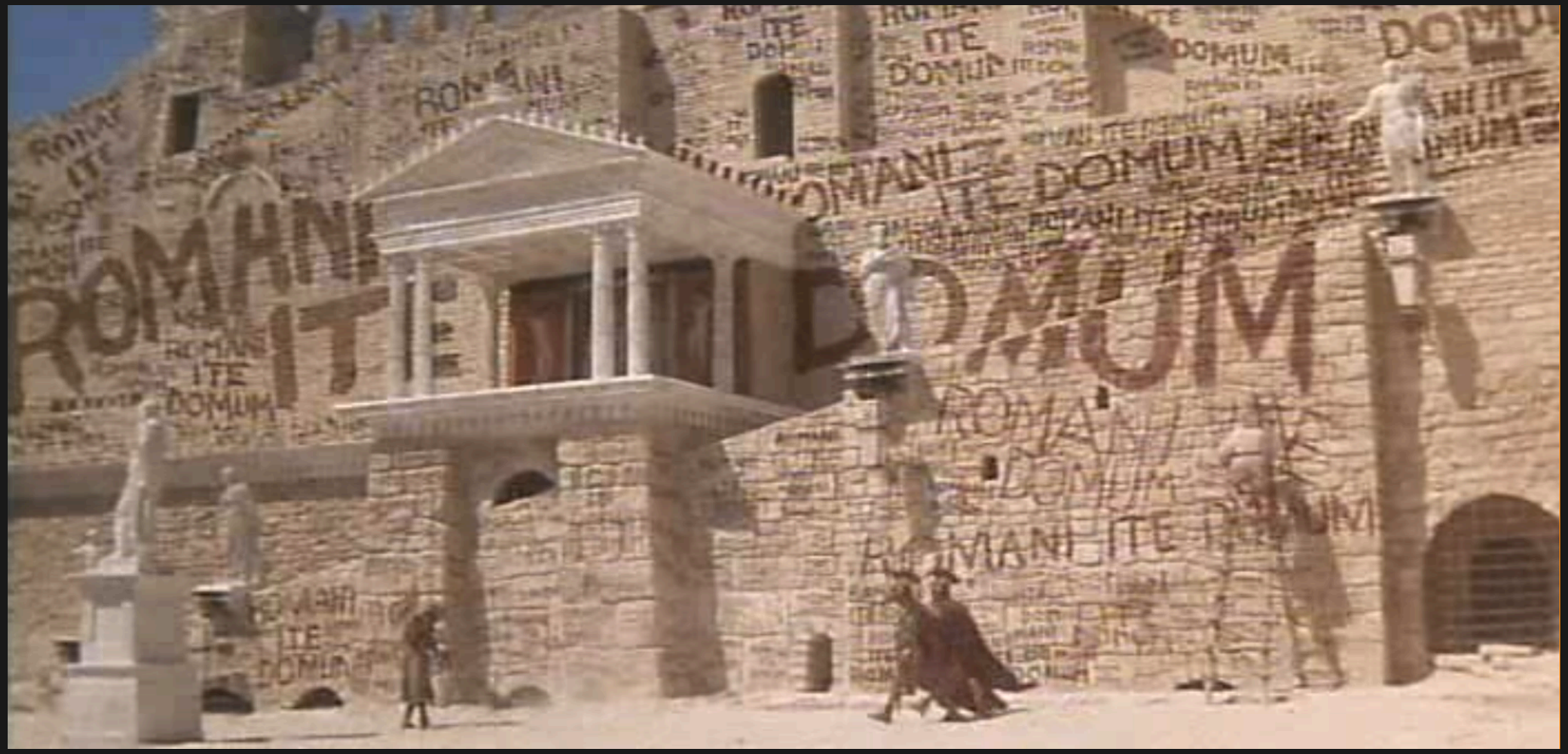
# ALERT CODE TSUNAMI

- Lots of C-style logic added
  - Different paradigms (e.g. error handling)
  - Little encapsulation
- Intertwined r2 and Ghidra state
  - E.g. current address
- No clear responsibilities
  - E.g. r4ghidra.repl.R4GhidraHttpHandler

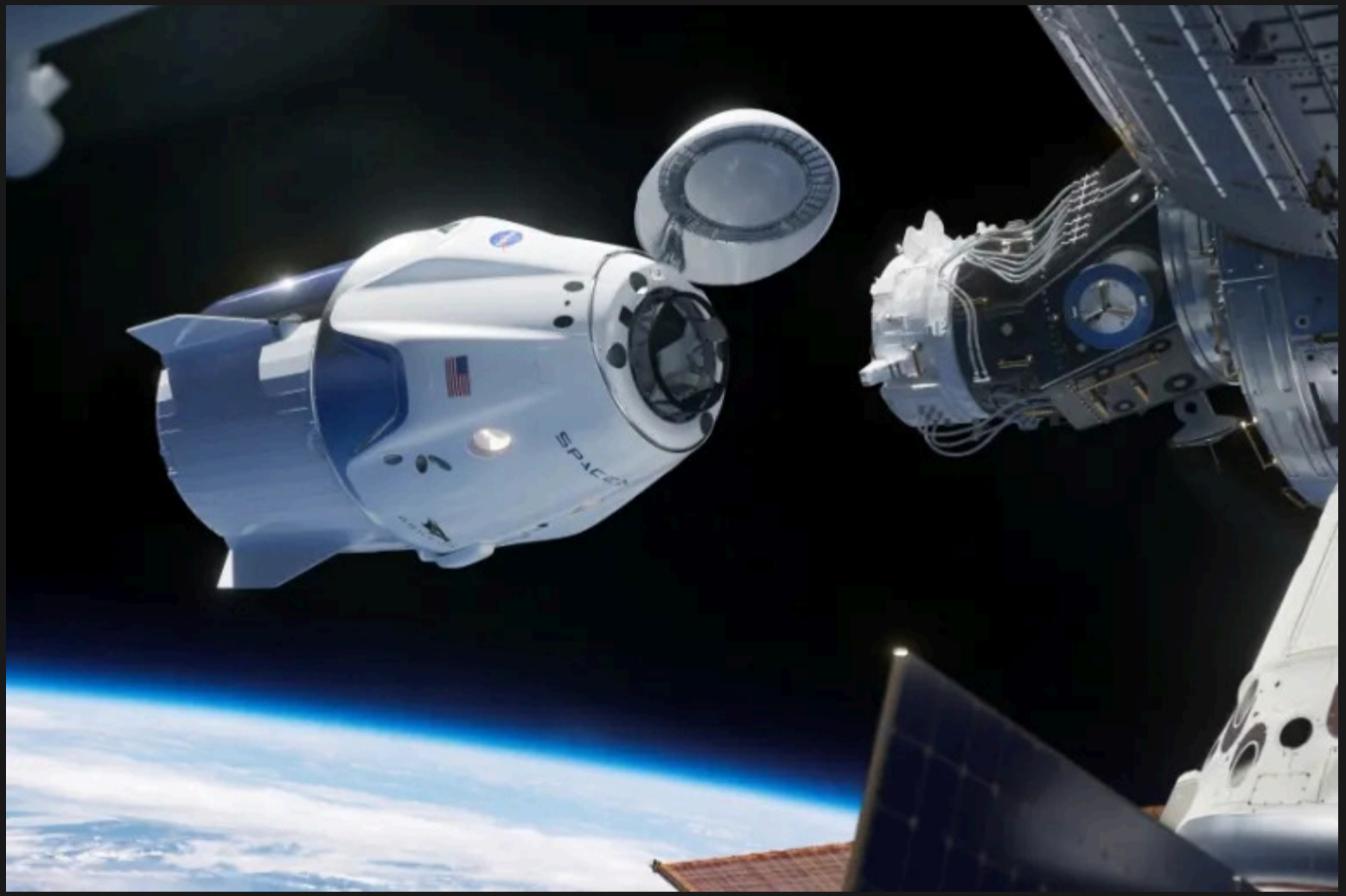
*"Software engineering is what happens to programming when you add time and other programmers." - Russ Cox*

# TESTS

# "WHEN IN ROME, DO AS THE ROMANS DO"



# ENCAPSULATION AND INTERFACES



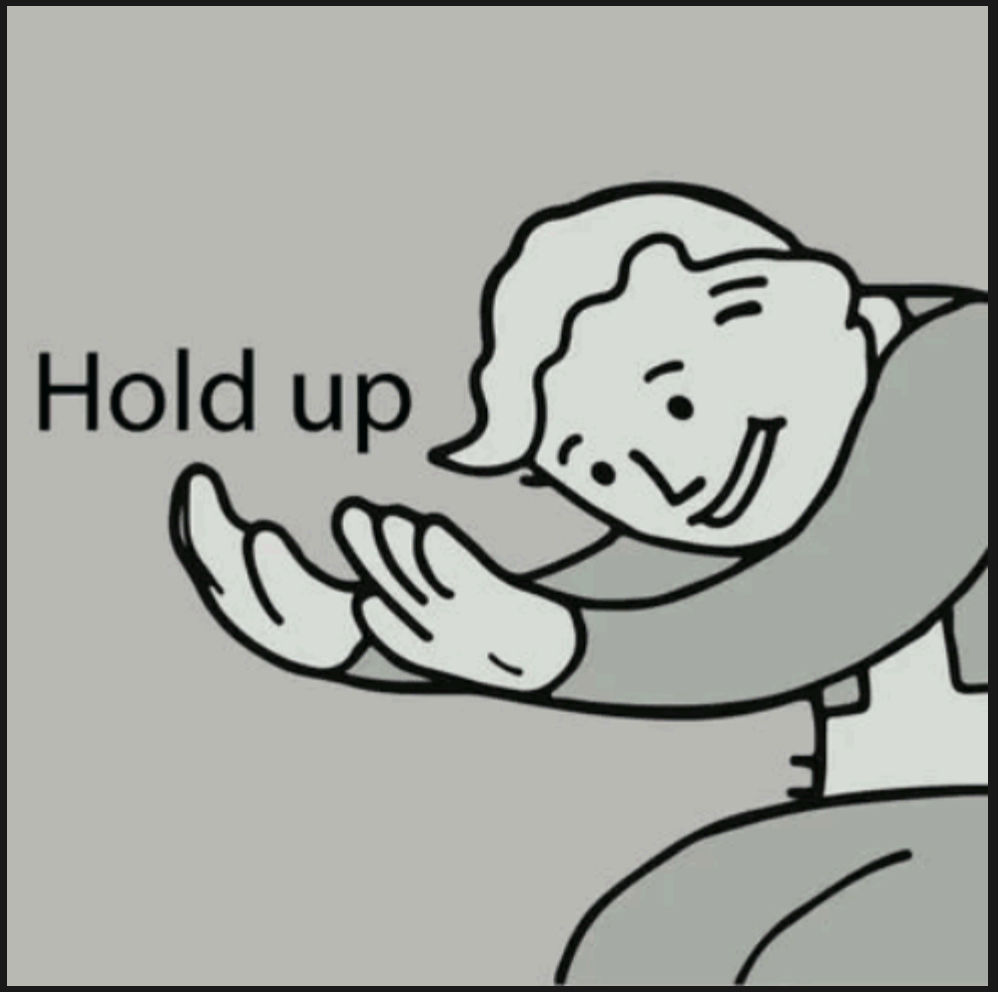
# GROW

- GUI-REPL sync
- JSON command handling
- r2web works again
  - Command handling still shared :)
- "Happy little surprise behaviors"

# REPL SURVEY

# THE REQUEST OF REQUESTS

*"Wouldn't it be great if I could transfer symbols between r2 and Ghidra?"*


Hold up

We are solving different problems!

# With **r2web** we can extend r2's features with external tools

HTTP is an extension protocol **for r2**

# With the **REPL** we bring r2's UX to Ghidra

A new UI **for Ghidra**

# Symbol porting is translation between API's

Should work **both ways**

What code *should* be writen?

# I'VE HEARD THIS BEFORE...

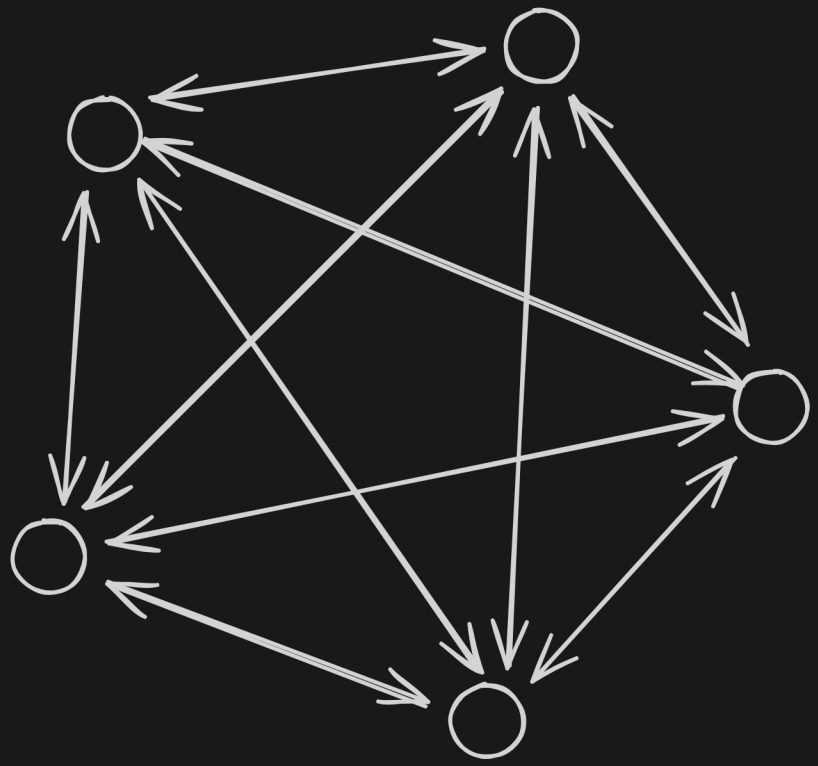
## Travis Goodspeed - Some Thoughts on Literate Disassembly and Symbol Porting

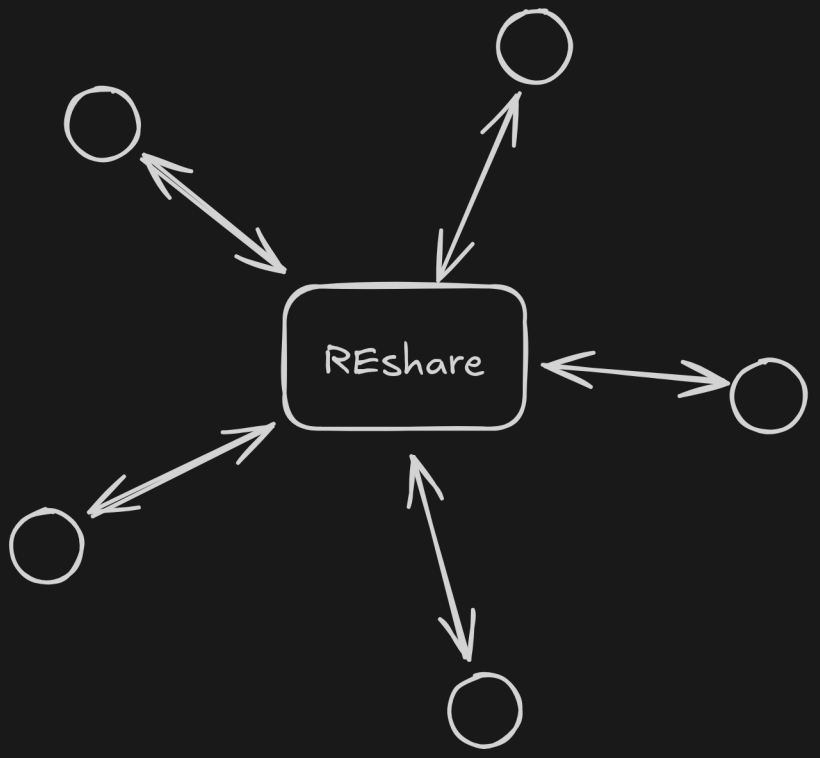
- We should have an *interchange format*
- Text files FTW
- r2 has been doing this right the whole time!

# RESHARE

- Reverse Engineering interchange format
- JSON based
  - *"This is JSON, I know this!"*
  - Great tooling and language support
  - ...
- (De)serializers can be generated from JSON Type Definition
  - Python, Java, Rust, JS, ...

# MORE THAN 0X3E8 WORDS





# PRINCIPLES

Perfect is the Enemy of Good

- "Release early, release often"
- Applying *some* information automatically is better than applying all manually
- Won't support *everything* (there can be variants though)

# PRINCIPLES

## Embrace redundancy

- Error Correction
- Diverse use-cases

# PRINCIPLES

You can fix it!

- Text format
- Intermediate processing (*jq* et al.)
- Typical users can code

# CURRENT CAPABILITIES

- Data Types
  - Primitive, Pointer, Structure, Enum, Union, Array
  - Function signatures
- Data and Function Symbols
  - Name, Address, Data Type

# CURRENT TOOLS

Python* prototypes

- Ghidra
  - Import/export data types and function prototypes
  - Import/export function symbols
- r2
  - Function symbol import
- PDB
  - Exporter based on pdbparse
  - Data types + function symbols

# RESHARE DEMO

RESHARE DEMO

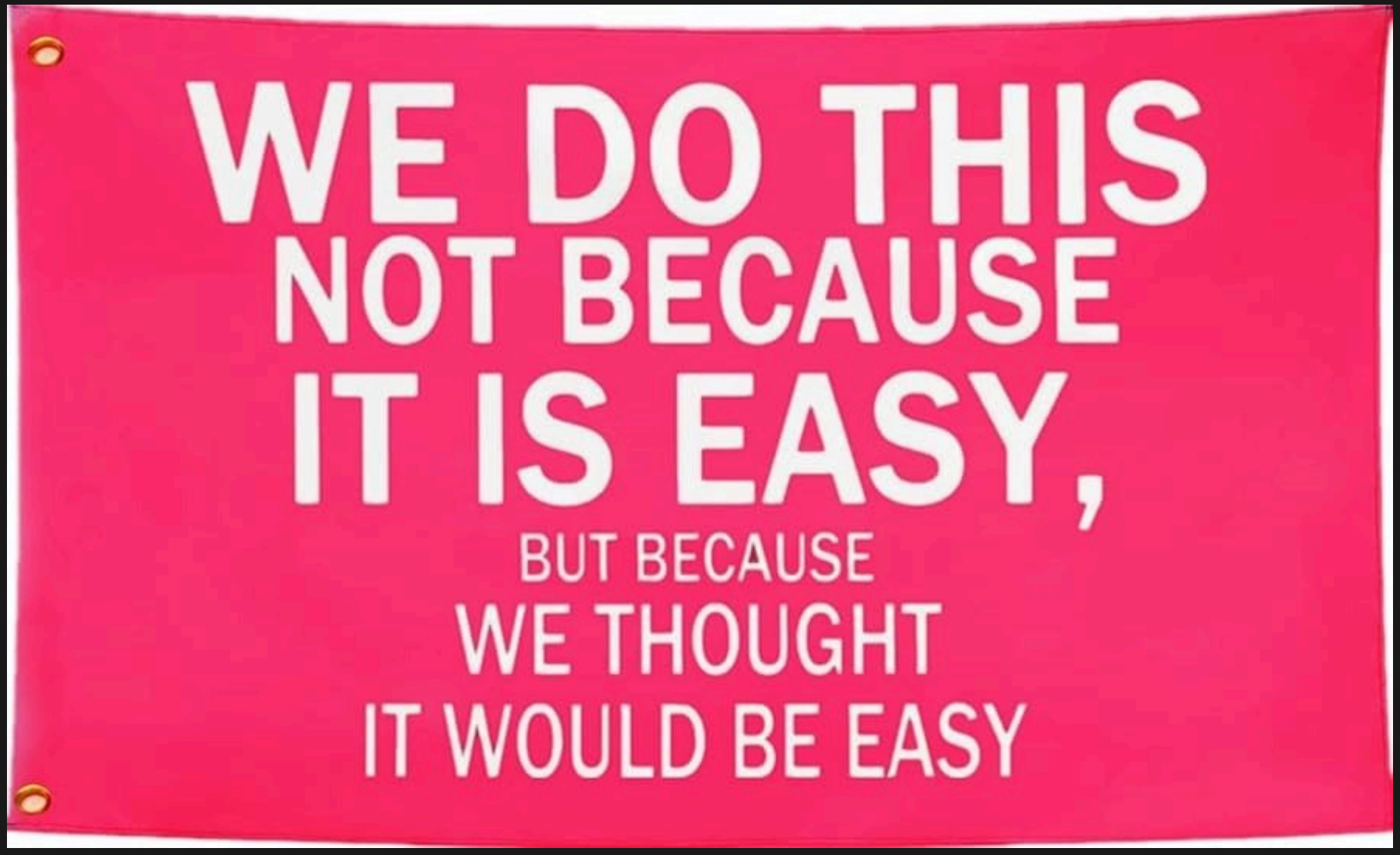
# OBVIOUS DIRECTIONS

- IDA support
- Binary ninja support
- BinExport support

# RESHARE SURVEY

# HELP WANTED

- Massive work
  - But we only have to do it once (per tool)
- Lots of glue tasks
- Dogfooding will reveal mistakes
  - Always pin library versions!


WE DO THIS
NOT BECAUSE
IT IS EASY,
BUT BECAUSE
WE THOUGHT
IT WOULD BE EASY

# THANK YOU!

https://github.com/radareorg/r4ghidra

https://github.com/v-p-b/reshare

Surveys

buherator at scrapco.de | @buherator@infosec.place