

**DRAPER**

# **Binary Analysis Tools in Cyber Testing**

John Merrill and Arch Owen

# PROBLEM STATEMENT

---

- Lack of source code in cyber engagements drives need for binary analysis tools, however...
- Binary-only analysis tools are limited and less developed than source analysis tools
- Draper has implemented **Modular, Open** software frameworks for static and dynamic analysis of **binary** code:
  - Dynamic analysis – VADER
  - Static analysis – SHREDDER.
- These frameworks allow for shared development and use by a broad contractor community.
- Draper has leveraged the inherent modularity of these frameworks to implement new advanced binary analysis capabilities.

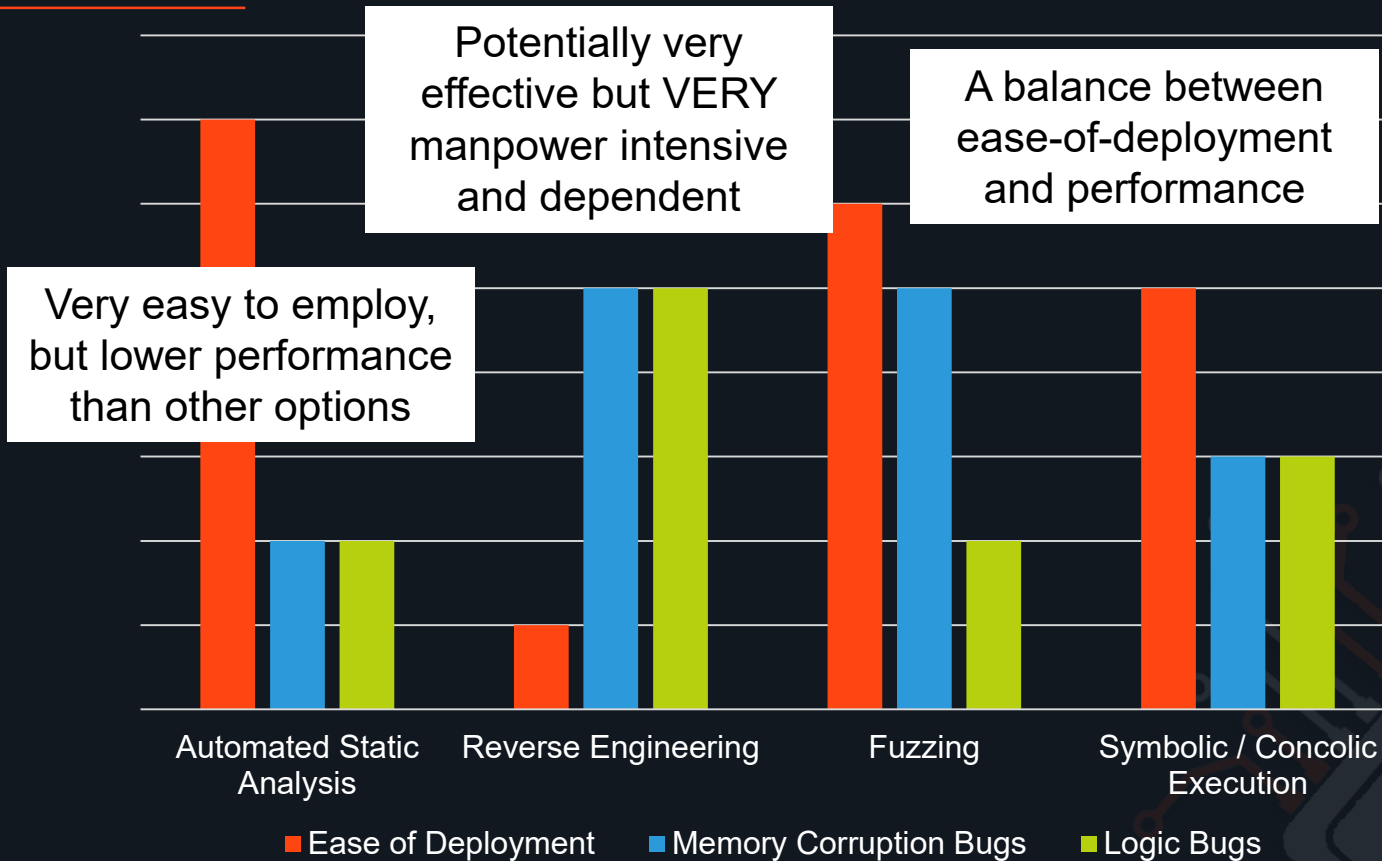
# SURVEY OF EXAMPLE BINARY TOOLS

Tool	Static Analysis		Dynamic Analysis			Usability/Adaptability				
	Automated Static Analysis	Reverse Engineering	Fuzzing	Symbolic / Concolic Execution	Multi-Platform	User Plugins	Automated	Open	Modular	Joint Use
CodeSonar	✓				✓		✓			
IDA		✓			✓	✓				
Ghidra		✓			✓	✓		✓	✓	
Binary Ninja		✓				✓				
AFL			✓				✓	✓		
Angr				✓	✓	✓	✓	✓		
Mayhem				✓	✓		✓			

Binary analysis tools exist BUT

- Few are open AND modular
- None are designed for joint use

# QUALITATIVE COMPARISON OF BINARY TOOLS

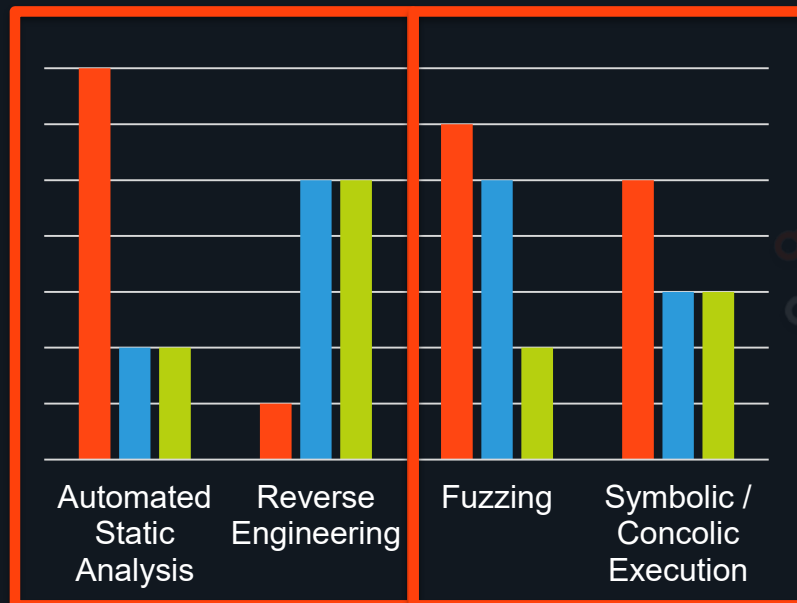


We need a means to efficiently leverage all techniques AND facilitate more rapid binary tool development and maturation.

# DRAPER'S APPROACH FOR RAPID TOOL DEVELOPMENT

- Rapid, robust tool development and maturation requires a 2-step approach
- Step 1: Develop a modular, open, automated framework
  - Automation: easy deployment
  - Modular and Open: easy development of new features
- Step 2: Rapidly develop and integrate novel techniques

SHREDDER  
Static Analysis



VADER  
Dynamic Analysis

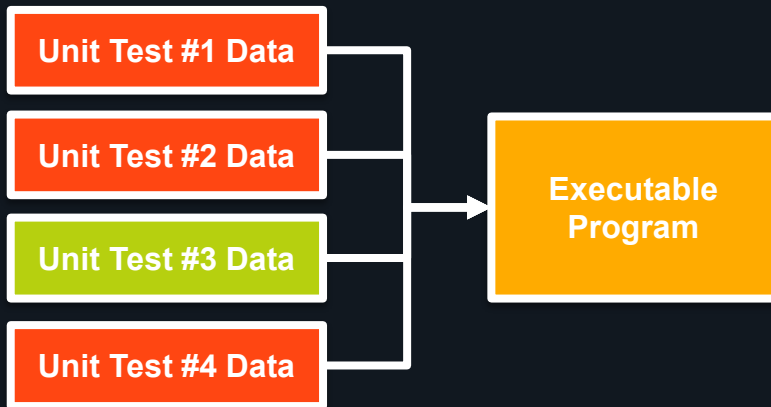
**DRAPER**

# **VADER Dynamic Analysis**

# WHAT IS FUZZING.....

Traditional software testing handles known edge cases. Fuzzing, in contrast, attempts to expose unknown edge cases through randomly generated tests.

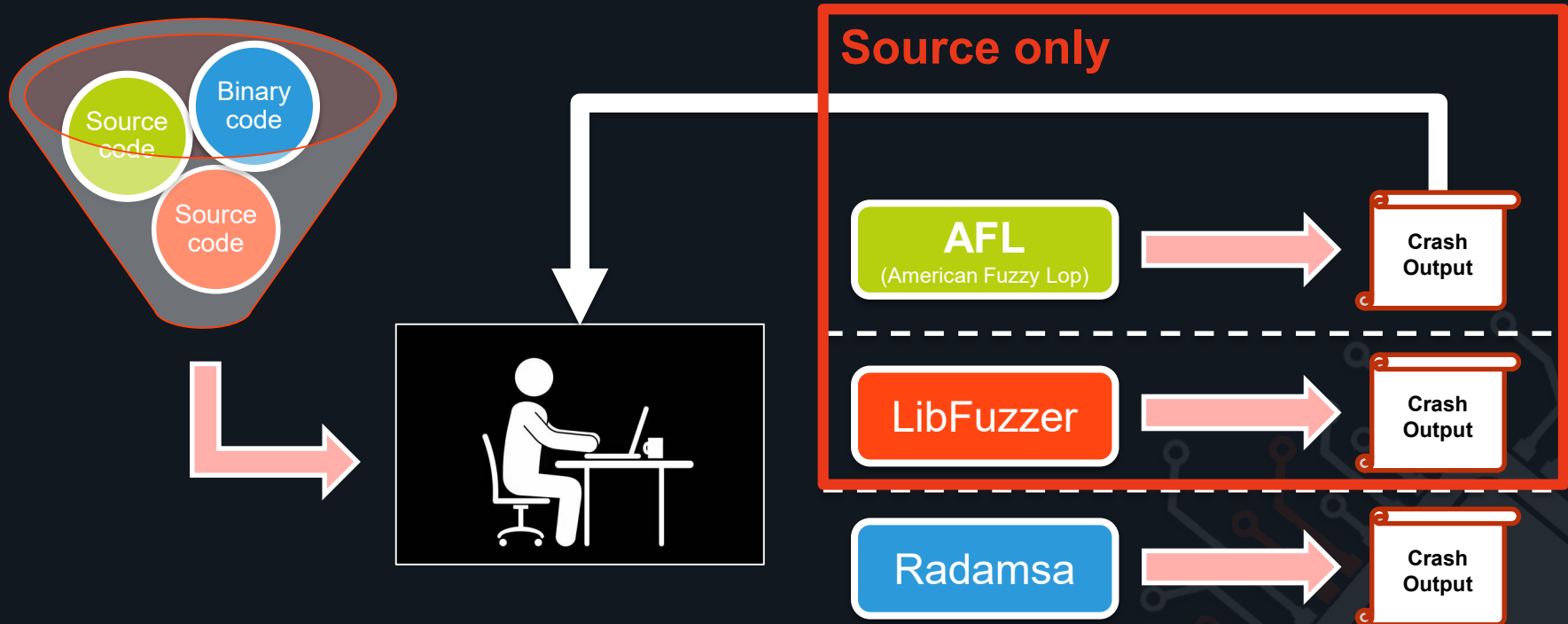
## Traditional Unit Testing



## Fuzzing Based Testing



# TRADITIONAL FUZZING LIMITATIONS

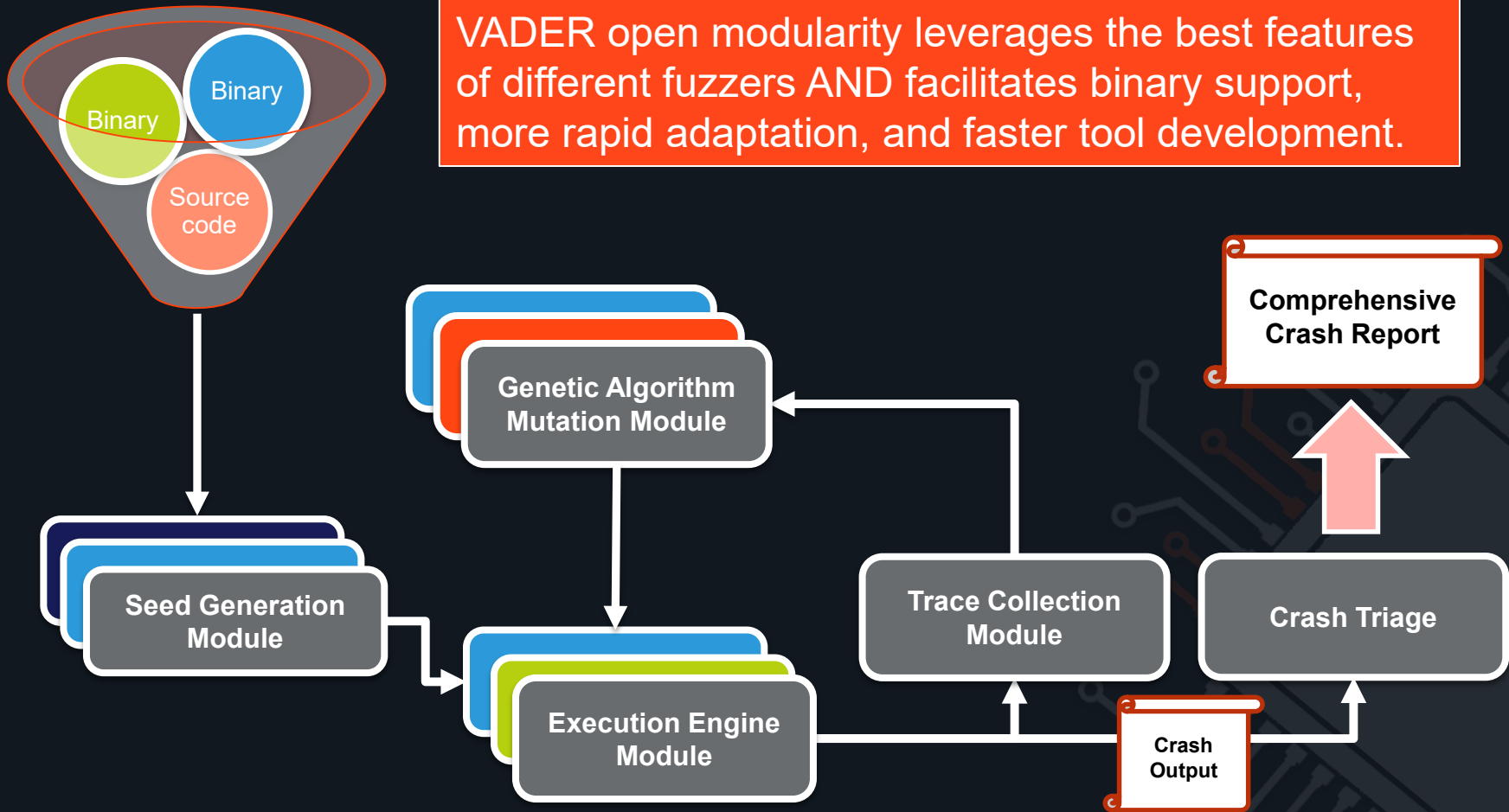


Fuzzers have tended to focus on source code, and the monolithic nature of available options limits innovation and advanced features.



# VADER MODULAR OPEN FUZZING FRAMEWORK

VADER open modularity leverages the best features of different fuzzers AND facilitates binary support, more rapid adaptation, and faster tool development.



# VADER CURRENT FEATURES

- Modular support for many existing open-source fuzzers
  - AFL
  - Radamsa
  - Domato
- Automated sample generation and crash triage

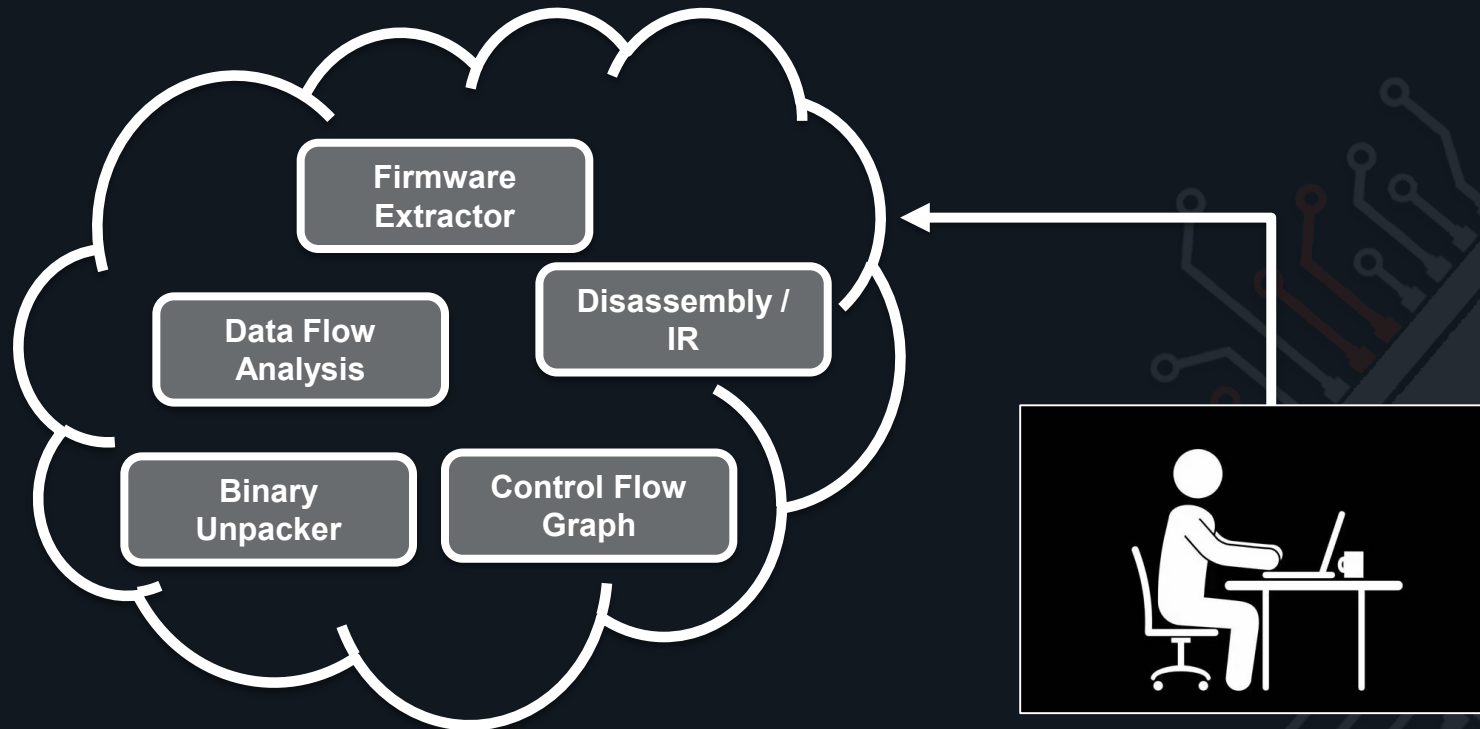
- Draper developed capabilities leveraging open modularity:
  - Custom Black Box Taint Tracking subsystem
    - Ability to traverse complex code paths
    - Full support for binary code
  - Real time, automated fuzzer switching - faster AND deeper code search

**DRAPER**

# **SHREDDER Static Analysis**

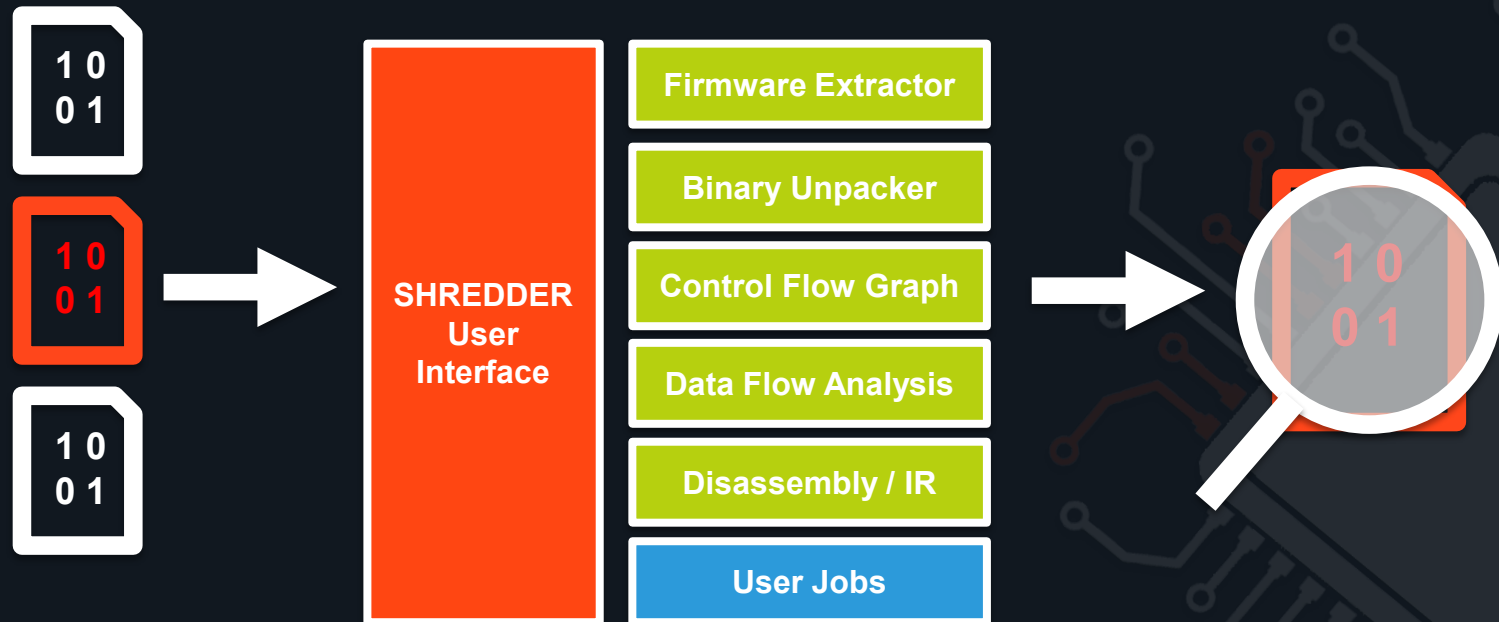
# LIMITATIONS TO REVERSE ENGINEERING

Reverse engineering is a time-consuming task involving numerous steps of information gathering. Many of these steps can be automated; however, the means to do so are limited.



# SHREDDER – STATIC ANALYSIS FRAMEWORK

The SHREDDER framework automates a large collection of common reverse engineering tasks and provides a simple interface for user extensions.



# SHREDDER CURRENT FEATURES

---

- Integration of numerous static analysis jobs
- IDA / Binary Ninja plugin support
- Draper developed capabilities leveraging open modularity:
  - Library Identification capability
    - Precise signature detection for library versions in binary
    - Correlation with CVE database

# PROBLEM STATEMENT

---

- Lack of source code in cyber engagements drives need for binary analysis tools, however...
- Binary-only analysis tools are limited and less developed than source analysis tools
- Draper has implemented **Modular, Open** software frameworks for static and dynamic analysis of **binary** code:
  - Dynamic analysis – VADER
  - Static analysis – SHREDDER.
- These frameworks allow for shared development and use by a broad contractor community.
- Draper has leveraged the inherent modularity of these frameworks to implement new advanced binary analysis capabilities.