

# **GeneVis:**

## **A Genealogical Visualization Tool for Directed Grey-box Fuzzing**

**Tae Eun Kim**

# Background

# Background

## Fuzzing

- Testing a program with randomly generated inputs

# Background

## Fuzzing

- Testing a program with randomly generated inputs
- Remarkable achievements
  - e.g., AFL, Google's OSS Fuzz project

# Background

## Fuzzing

- Testing a program with randomly generated inputs
- Remarkable achievements
  - e.g., AFL, Google's OSS Fuzz project

## Directed Grey-box Fuzzing

# Background

## Fuzzing

- Testing a program with randomly generated inputs
- Remarkable achievements
  - e.g., AFL, Google's OSS Fuzz project

## Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)

# Background

## Fuzzing

- Testing a program with randomly generated inputs
- Remarkable achievements
  - e.g., AFL, Google's OSS Fuzz project

## Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program

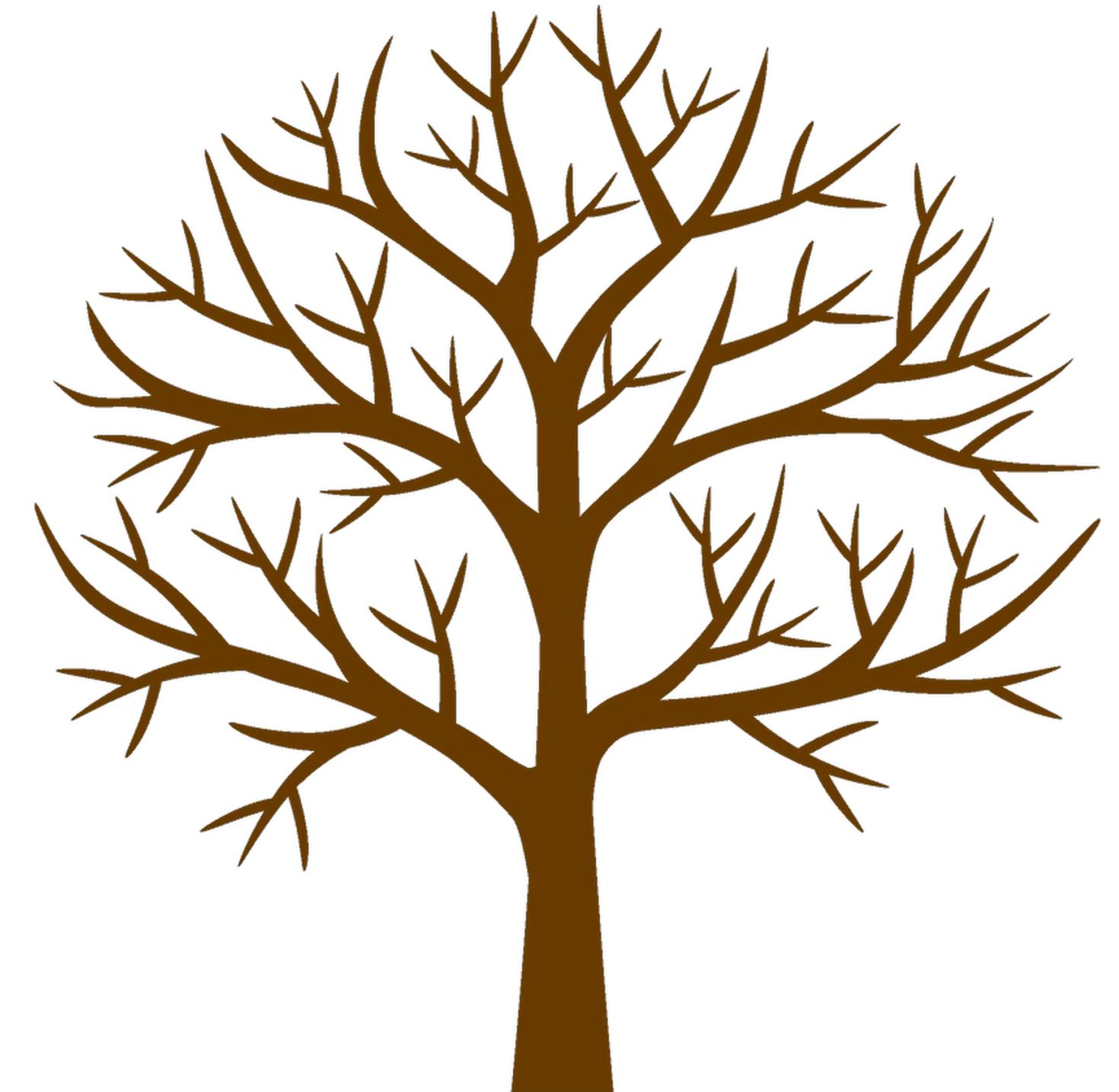
# Background

## Fuzzing

- Testing a program with randomly generated inputs
- Remarkable achievements
  - e.g., AFL, Google's OSS Fuzz project

## Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program



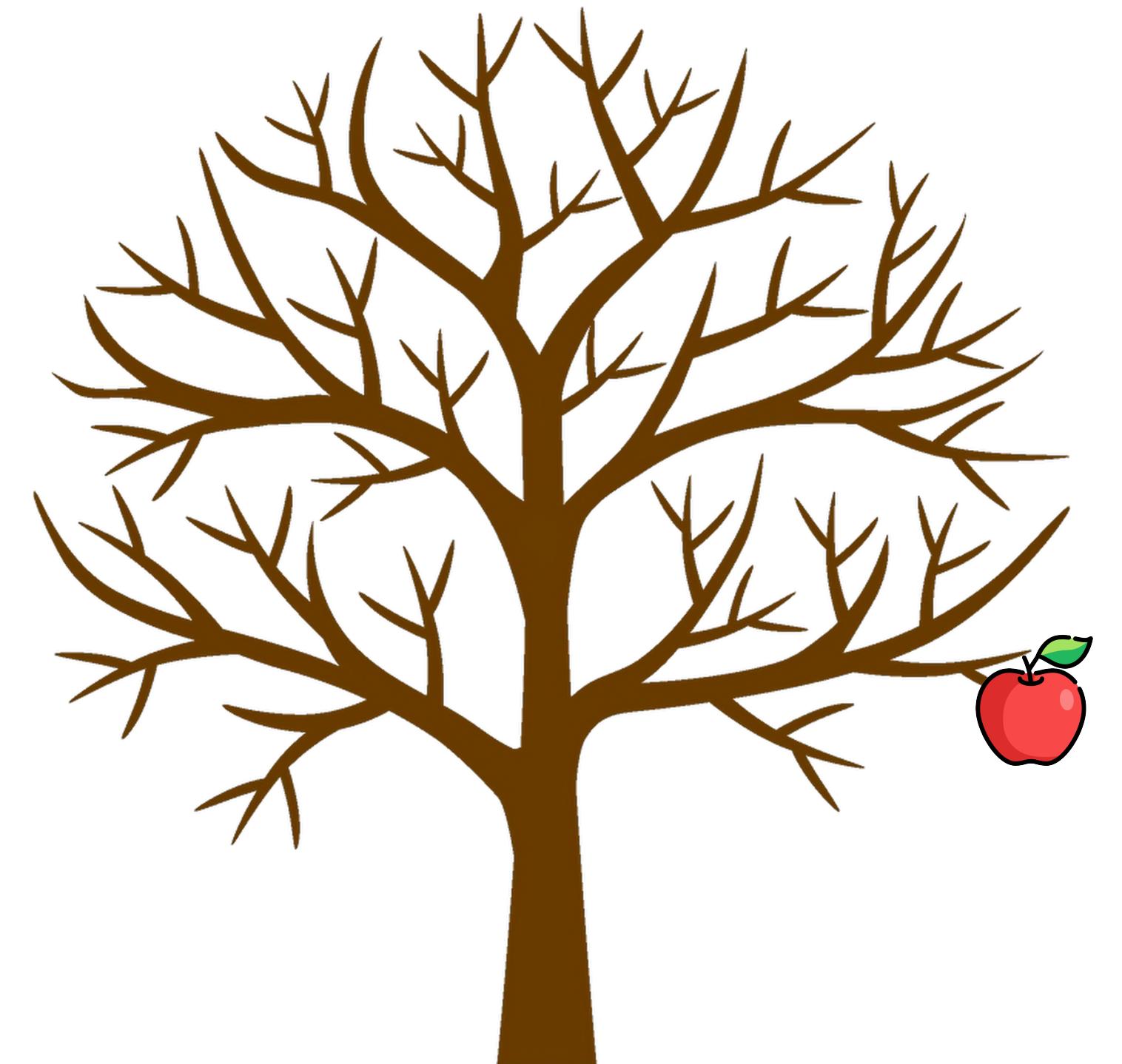
# Background

## Fuzzing

- Testing a program with randomly generated inputs
- Remarkable achievements
  - e.g., AFL, Google's OSS Fuzz project

## Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program



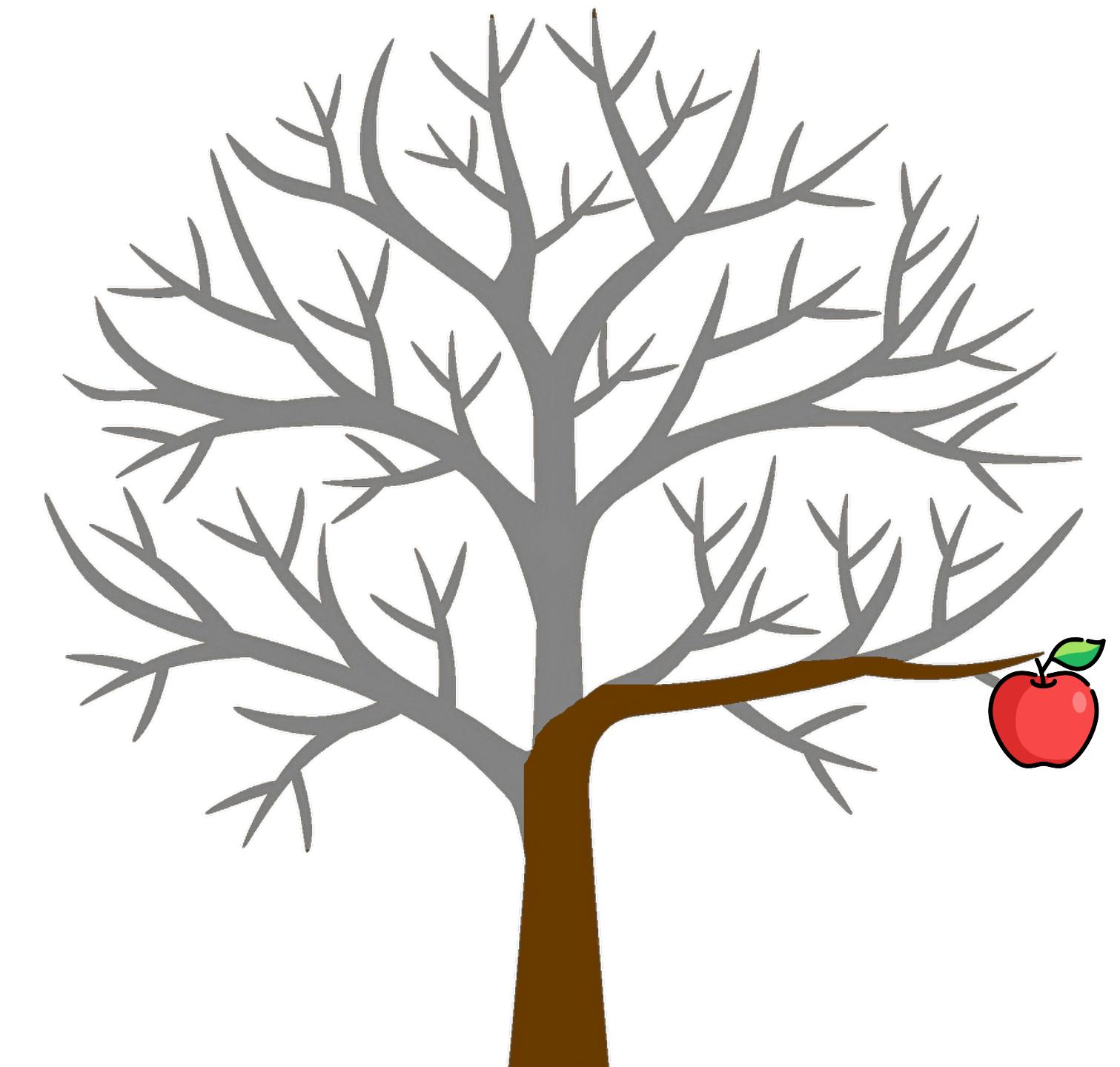
# Background

## Fuzzing

- Testing a program with randomly generated inputs
- Remarkable achievements
  - e.g., AFL, Google's OSS Fuzz project

## Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program



# Grey-box Fuzzing

# Grey-box Fuzzing

Fuzzer



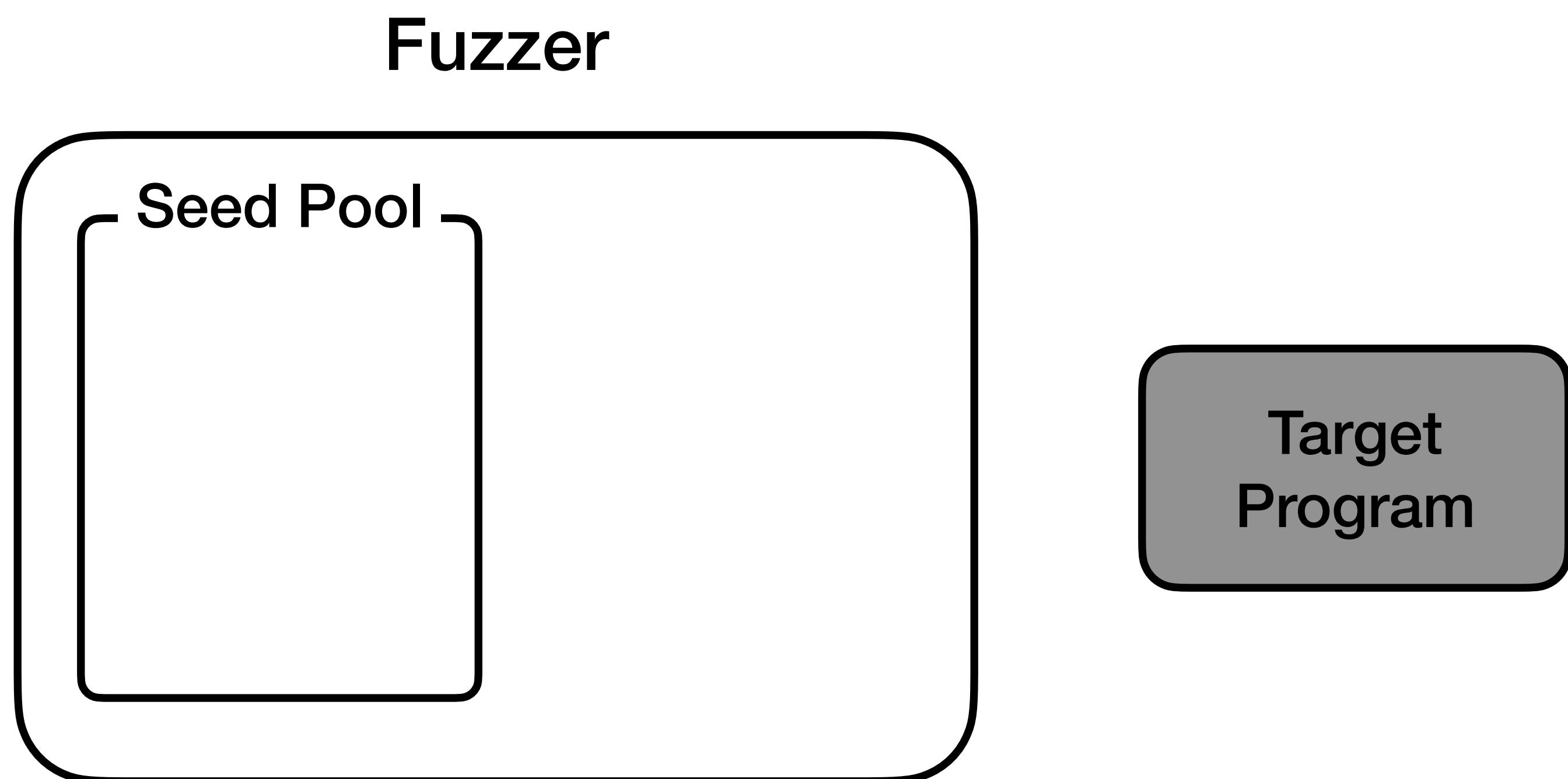
# Grey-box Fuzzing

Fuzzer

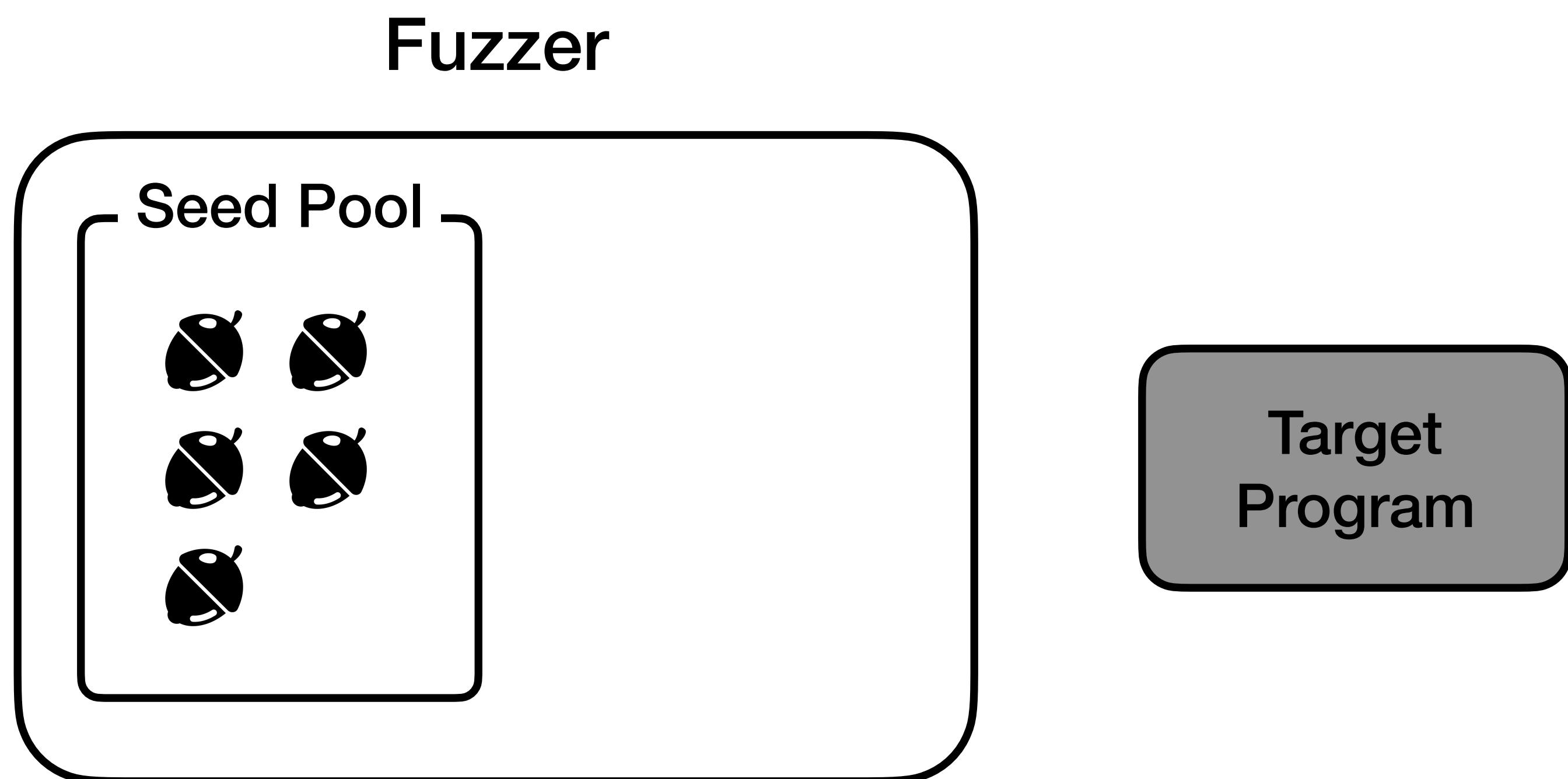


Target  
Program

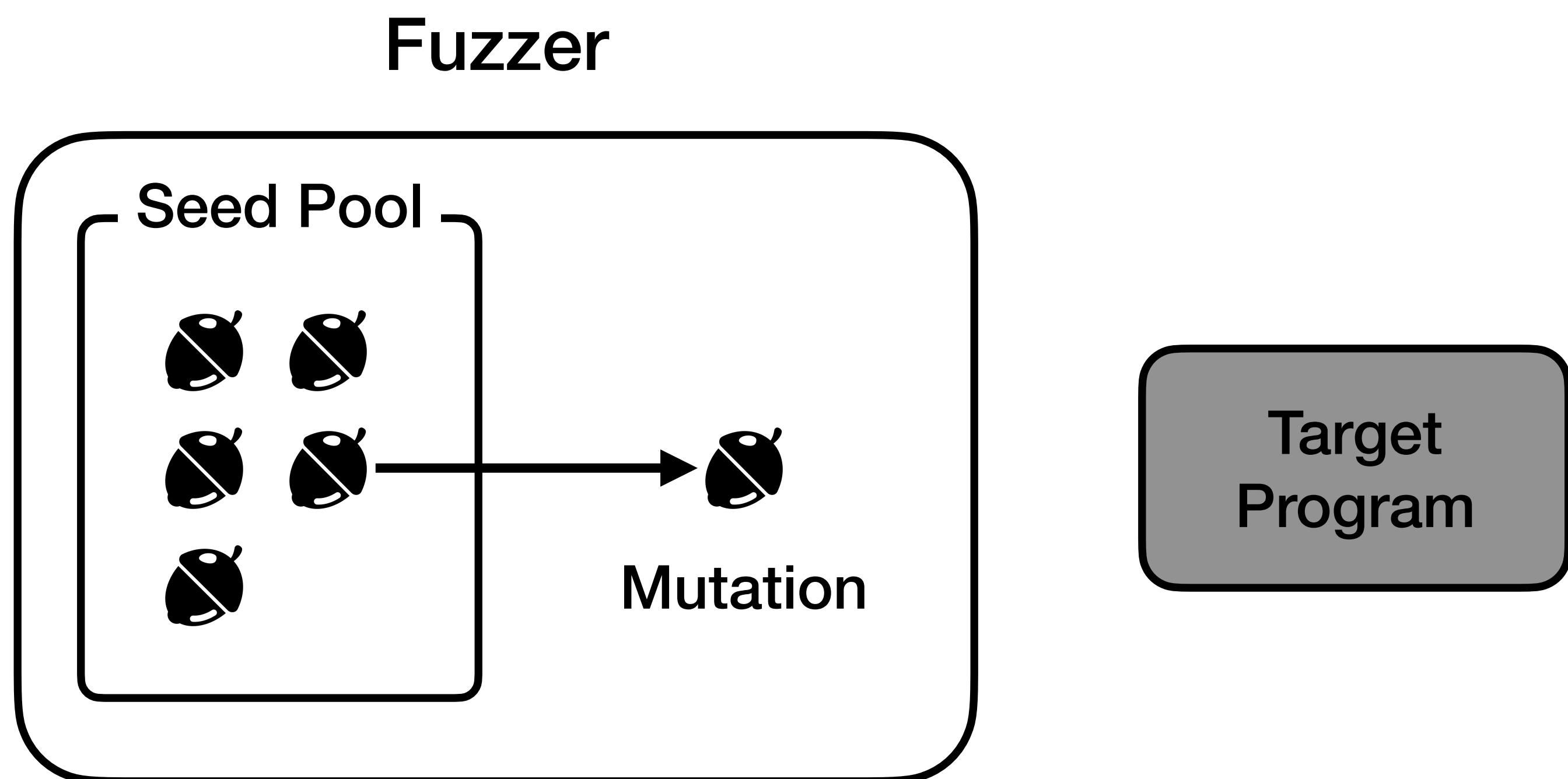
# Grey-box Fuzzing



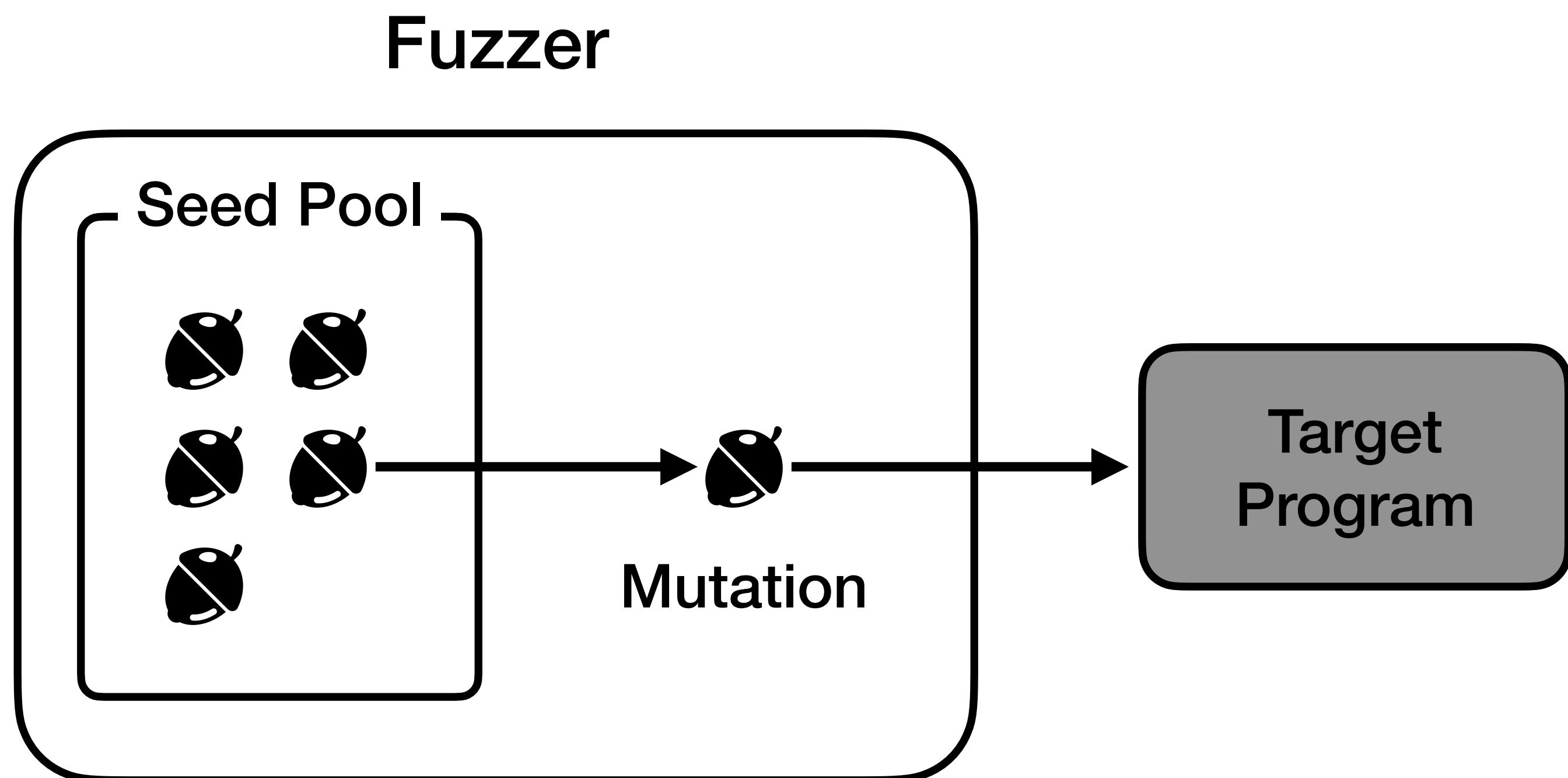
# Grey-box Fuzzing



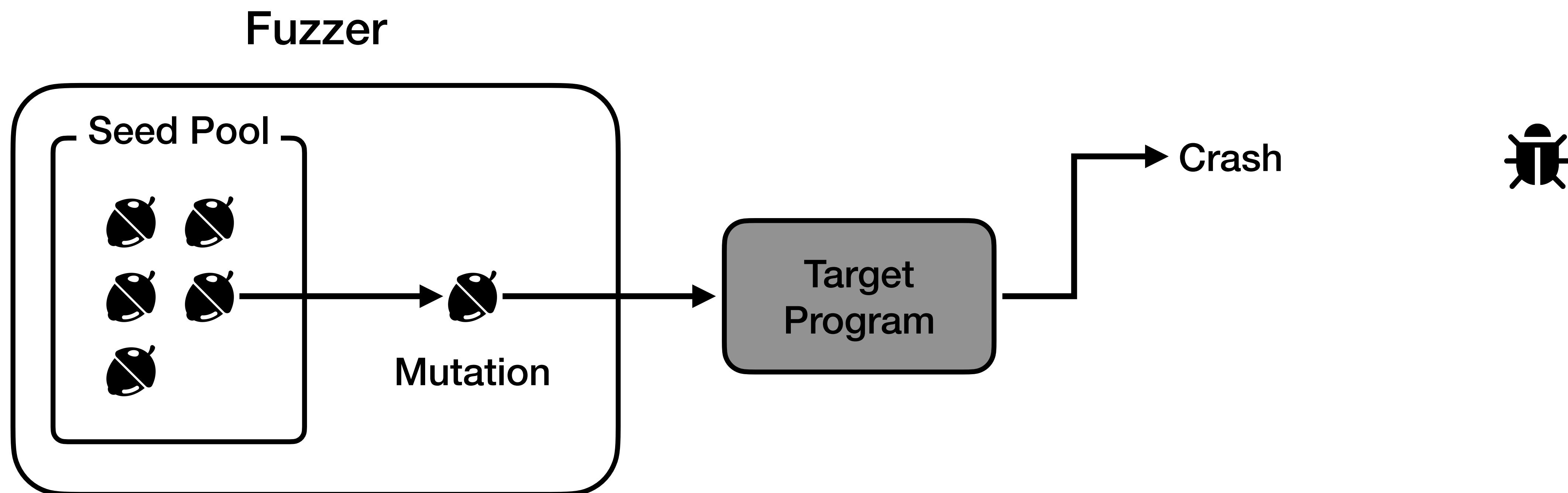
# Grey-box Fuzzing



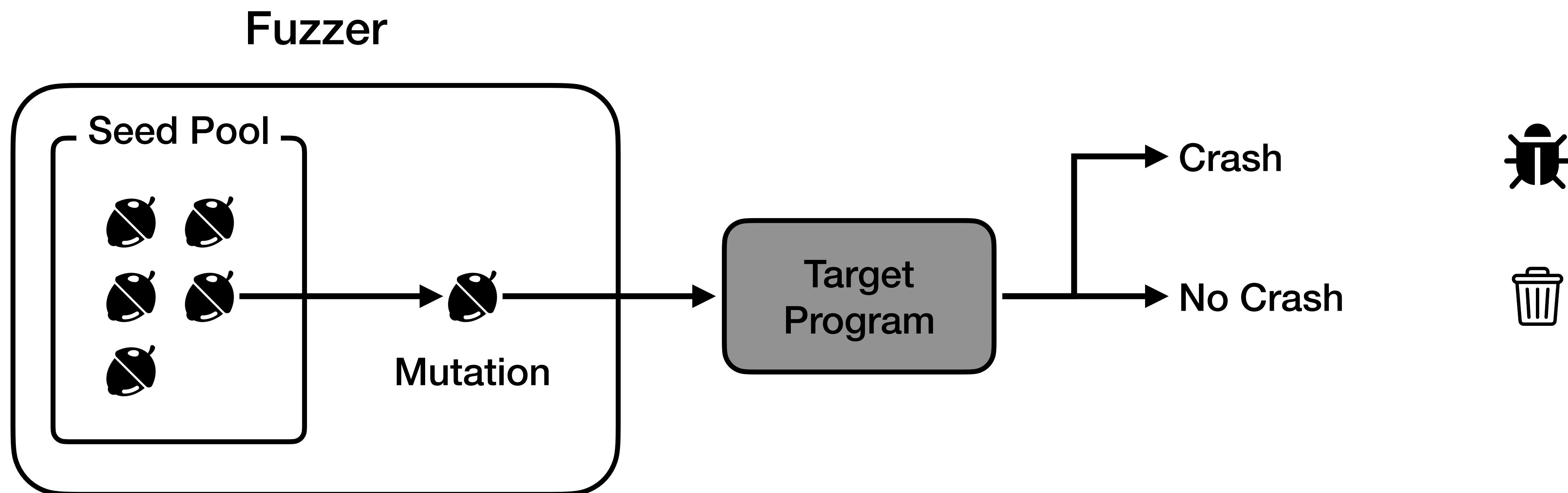
# Grey-box Fuzzing



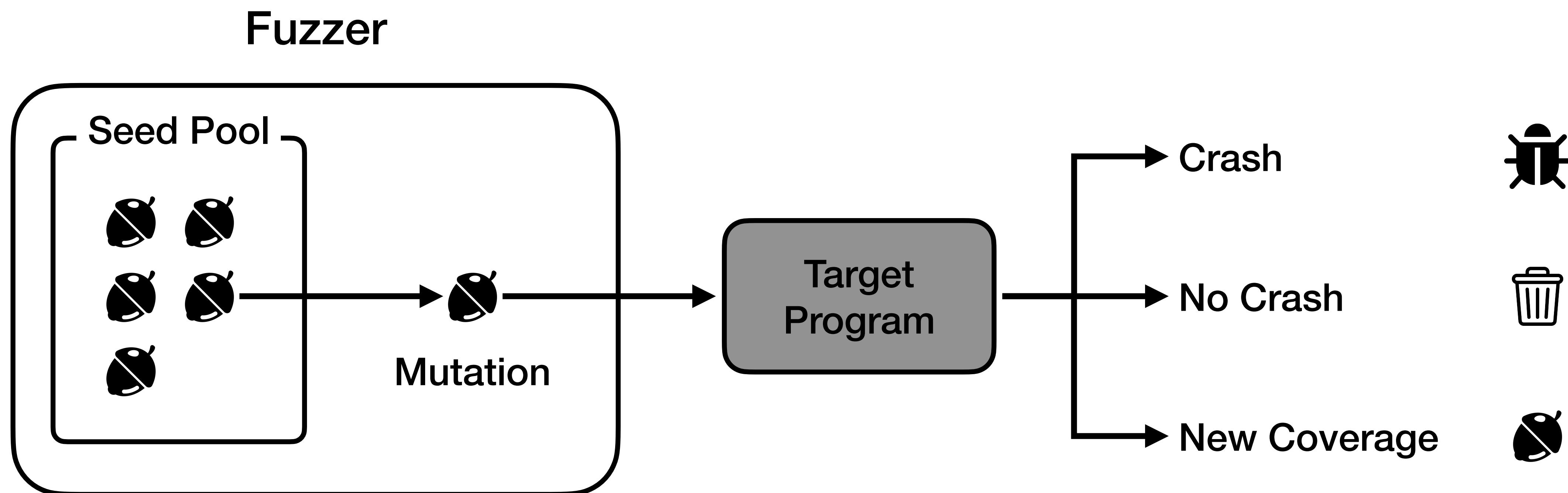
# Grey-box Fuzzing



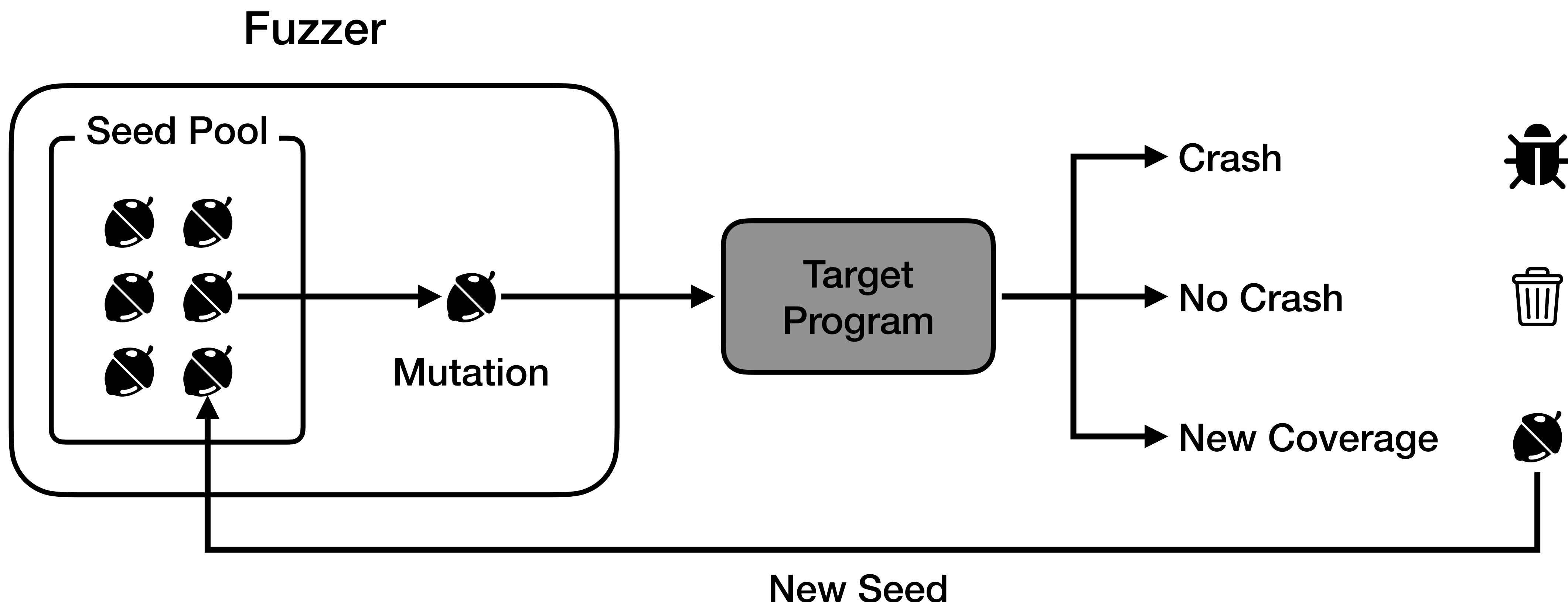
# Grey-box Fuzzing



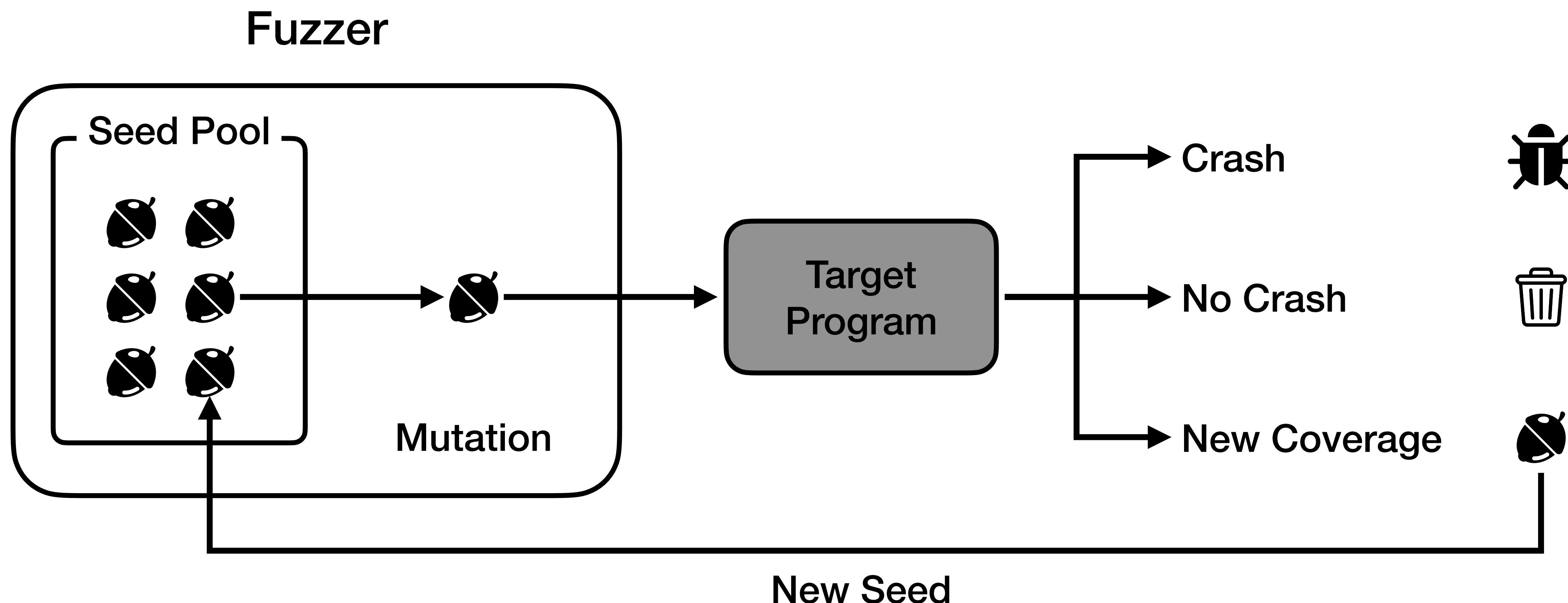
# Grey-box Fuzzing



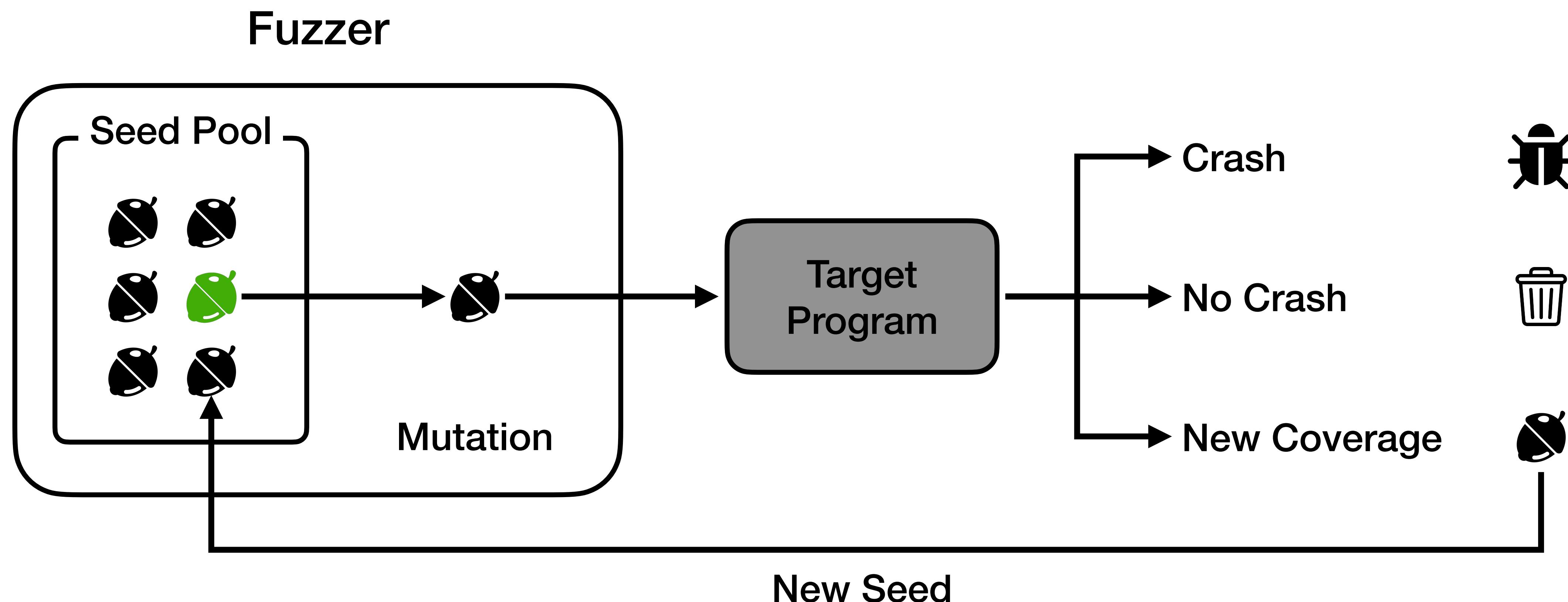
# Grey-box Fuzzing



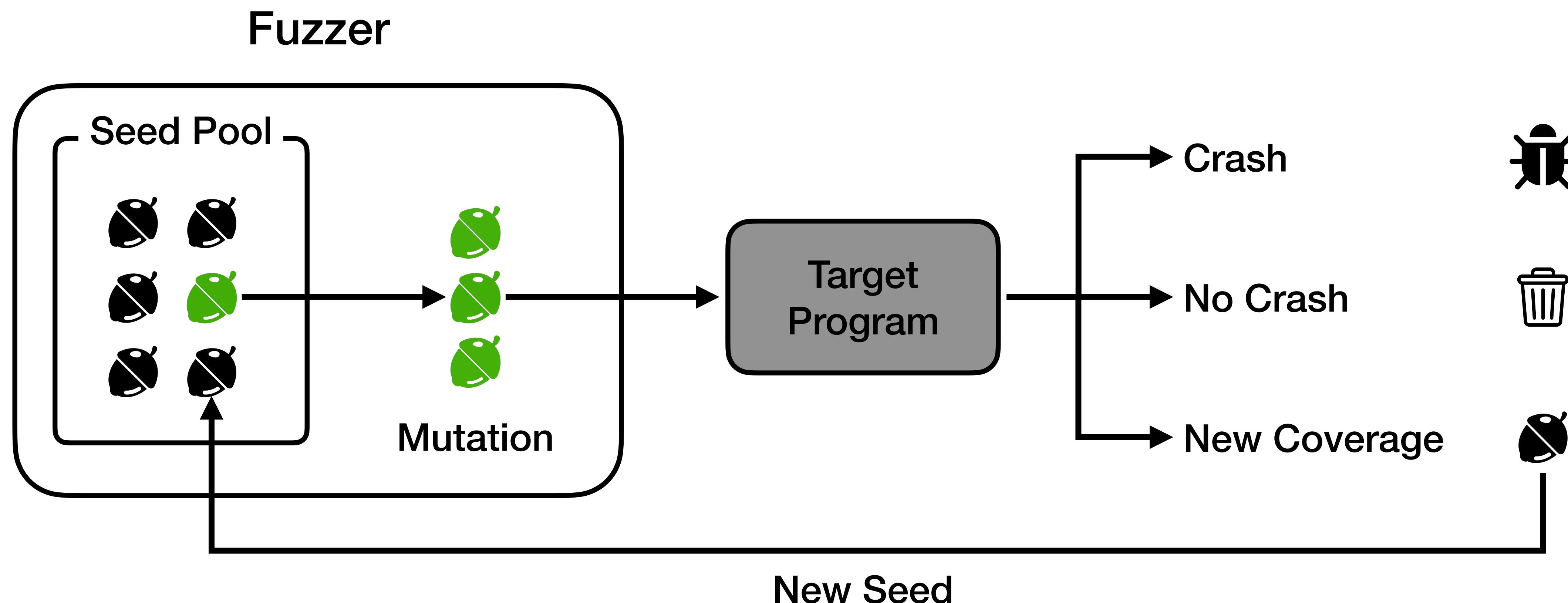
# Directed Grey-box Fuzzing



# Directed Grey-box Fuzzing



# Directed Grey-box Fuzzing



# Analysis of Directed Grey-box Fuzzing

# **Analysis of Directed Grey-box Fuzzing**

## **Progress of Fuzzing**

# **Analysis of Directed Grey-box Fuzzing**

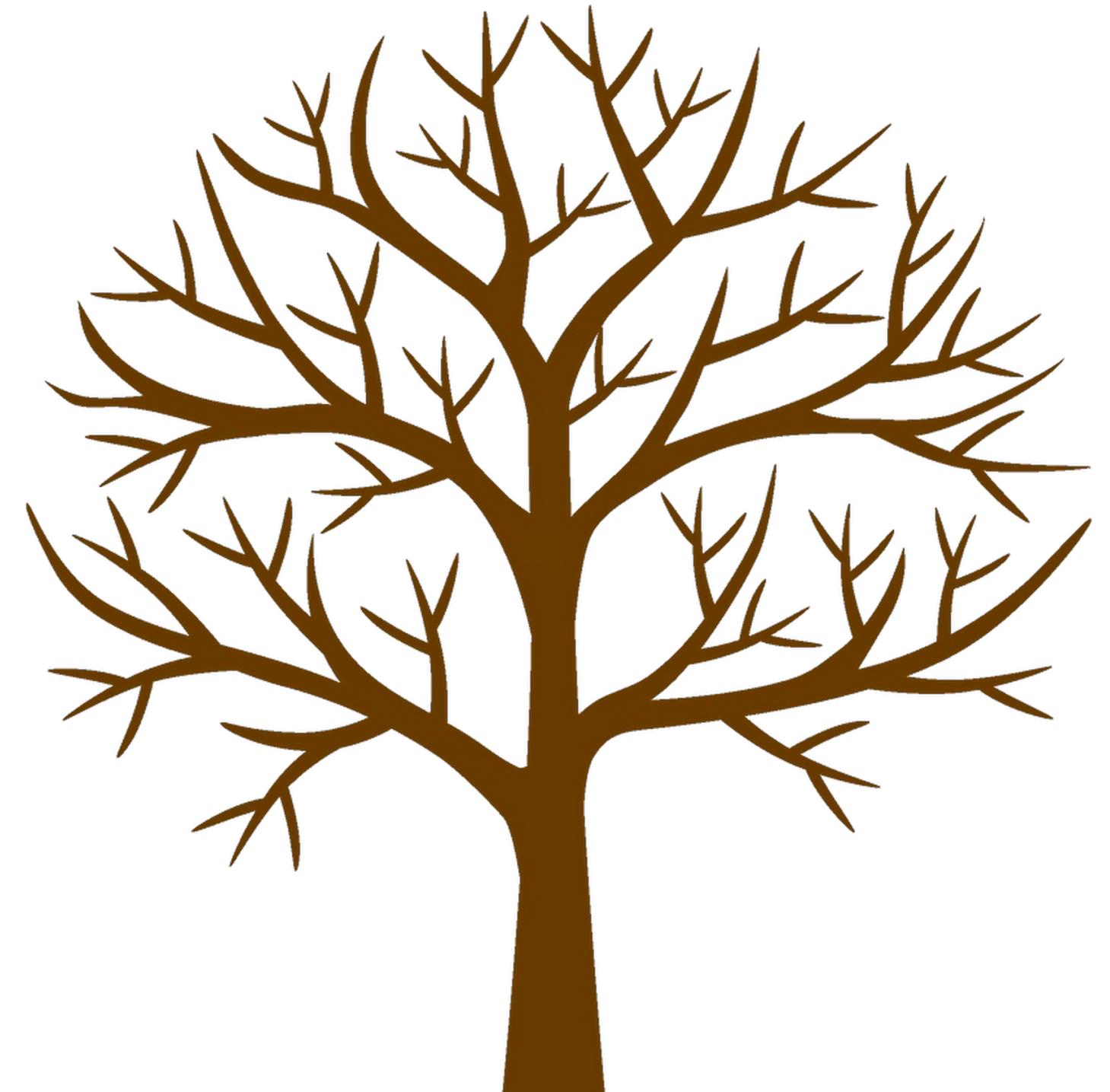
## **Progress of Fuzzing**

- Each seed represents each step into the program

# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

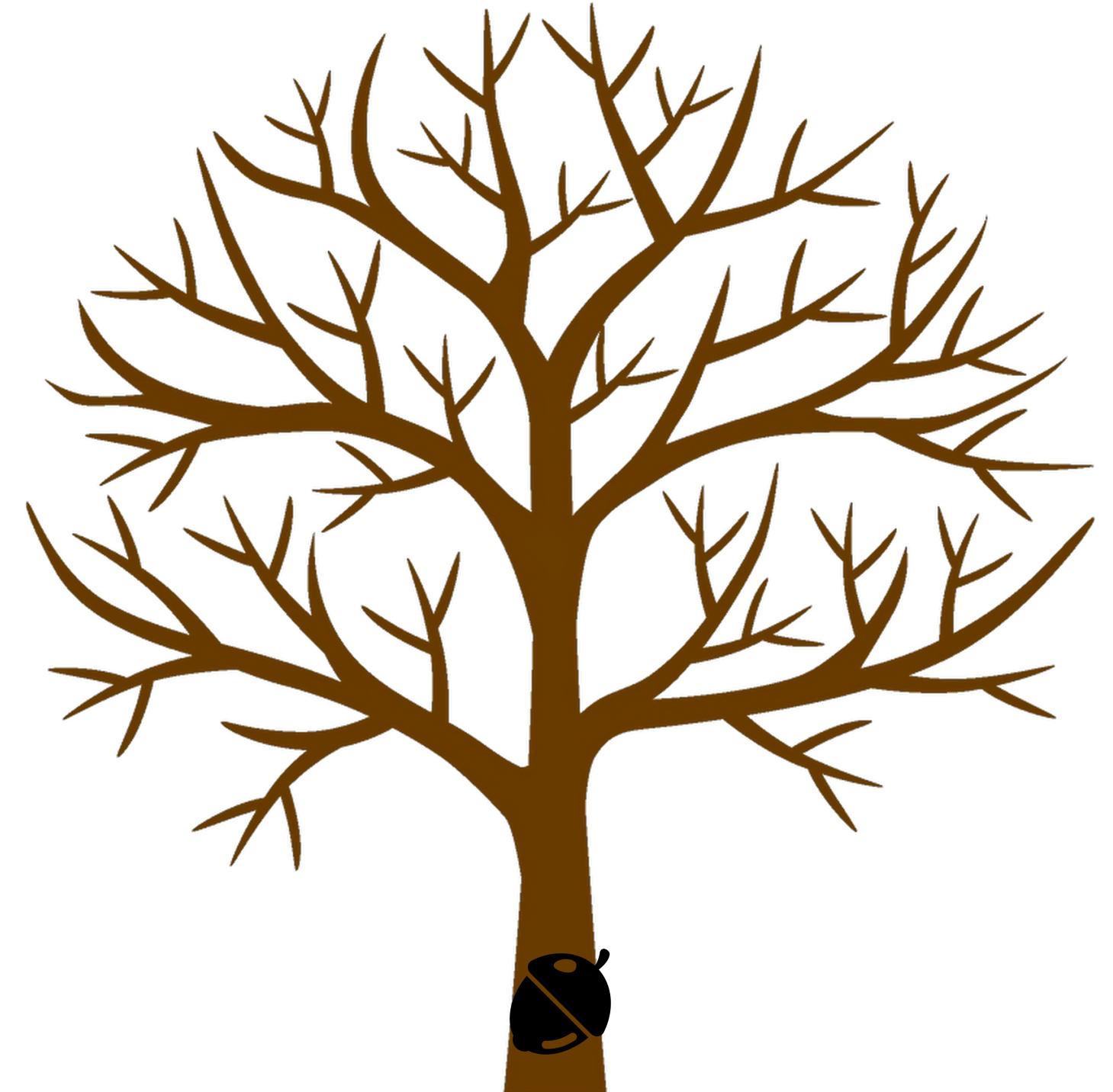
- Each seed represents each step into the program



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

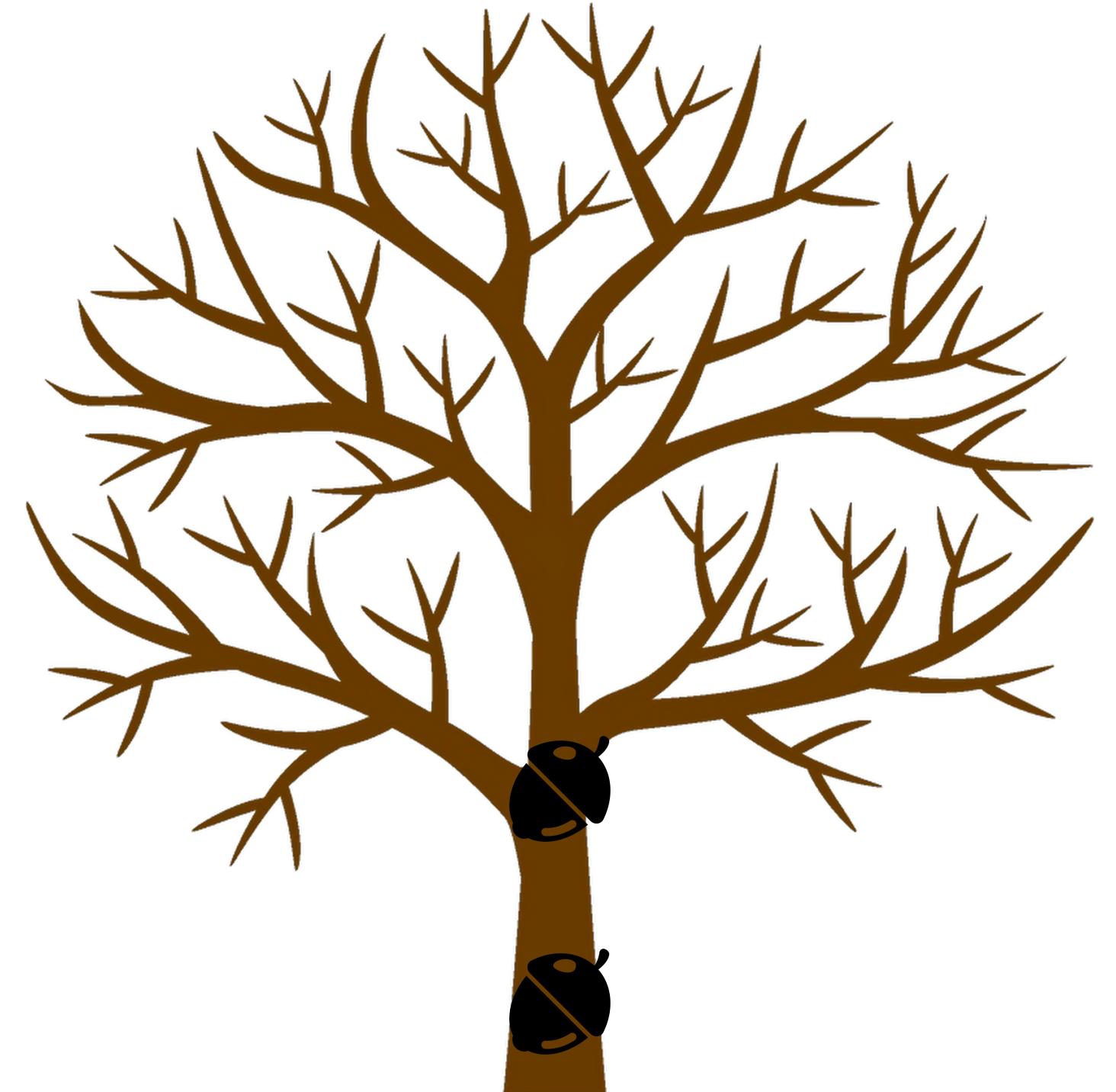
- Each seed represents each step into the program



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

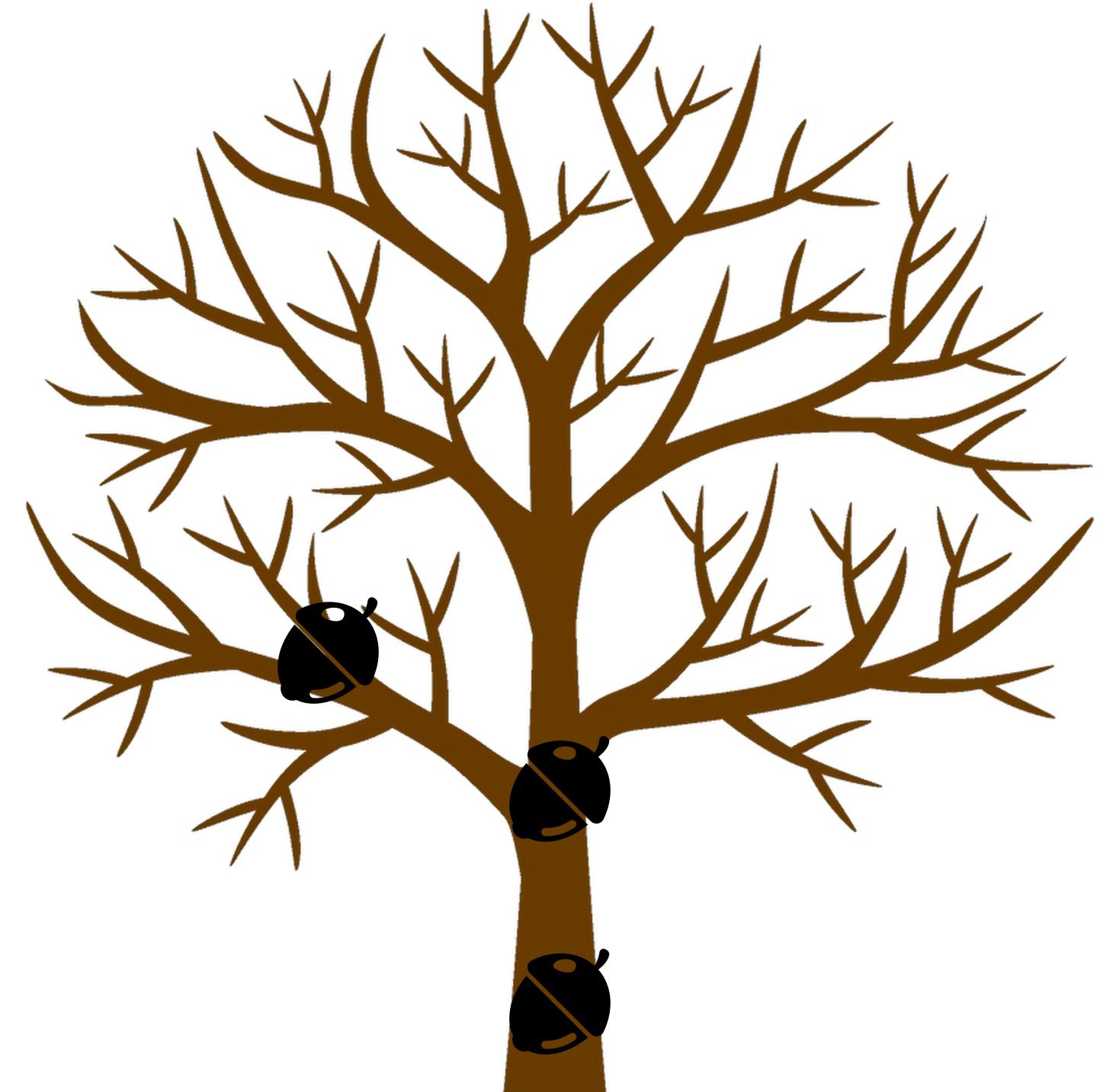
- Each seed represents each step into the program



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

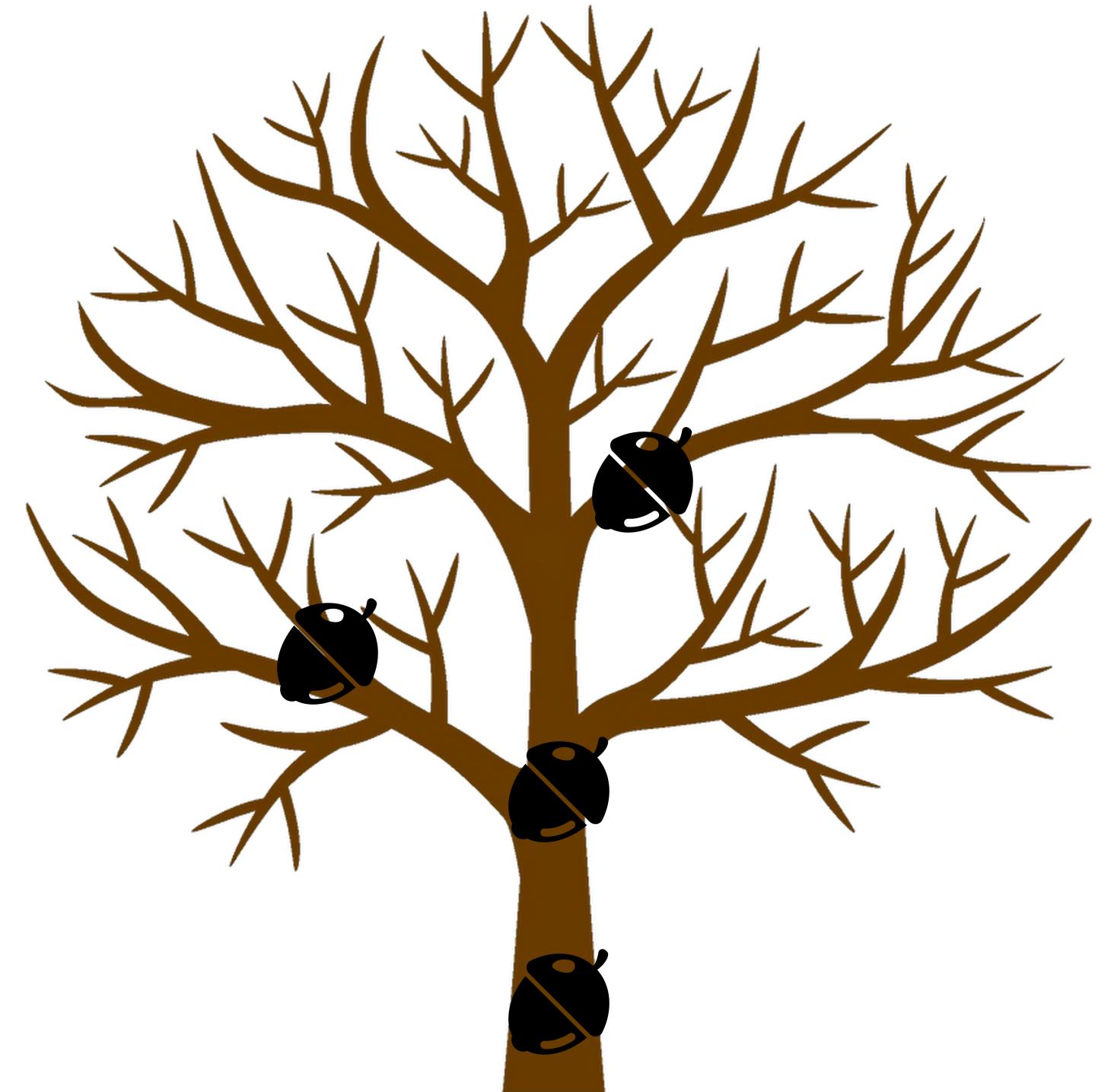
- Each seed represents each step into the program



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

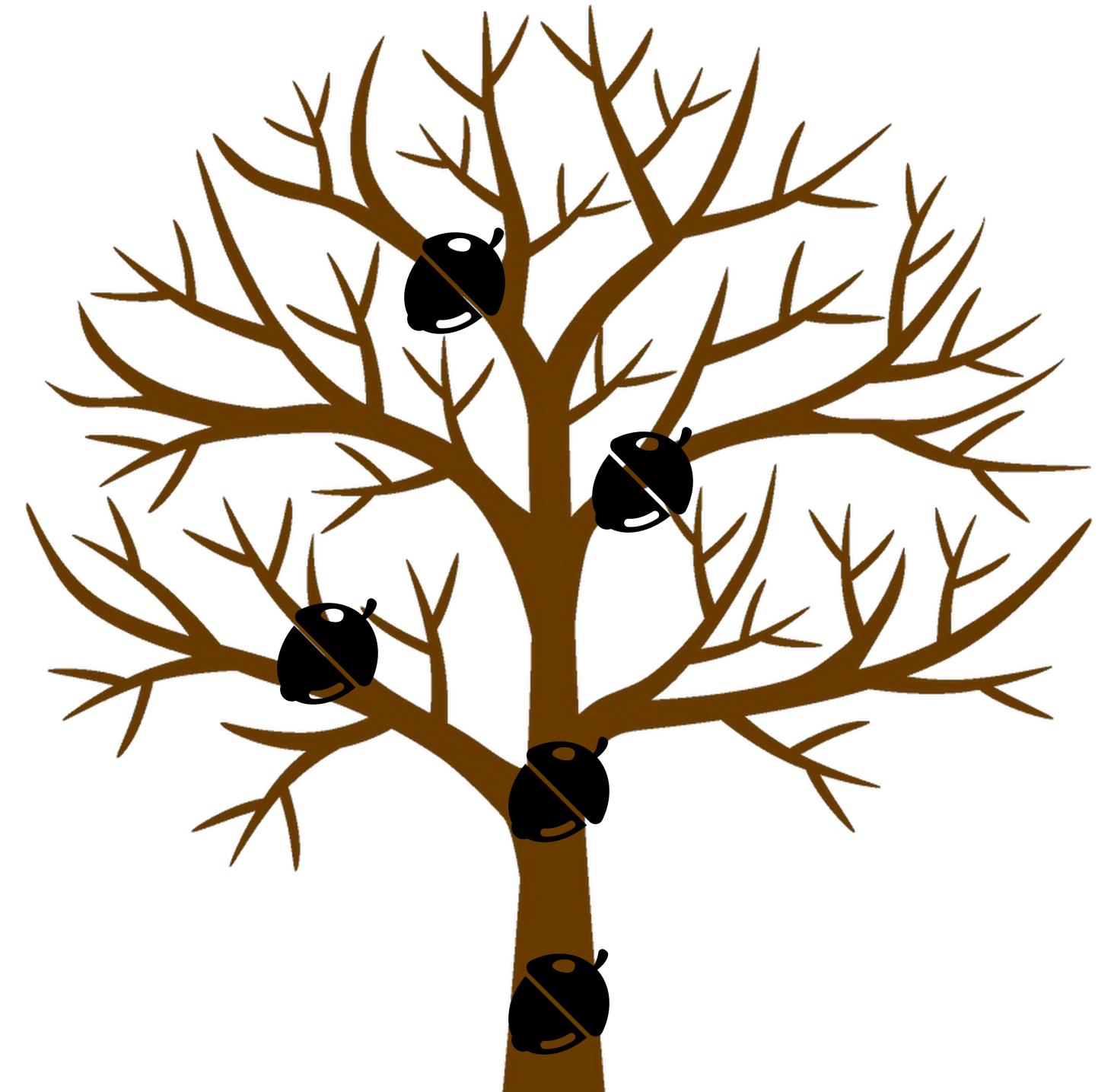
- Each seed represents each step into the program



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

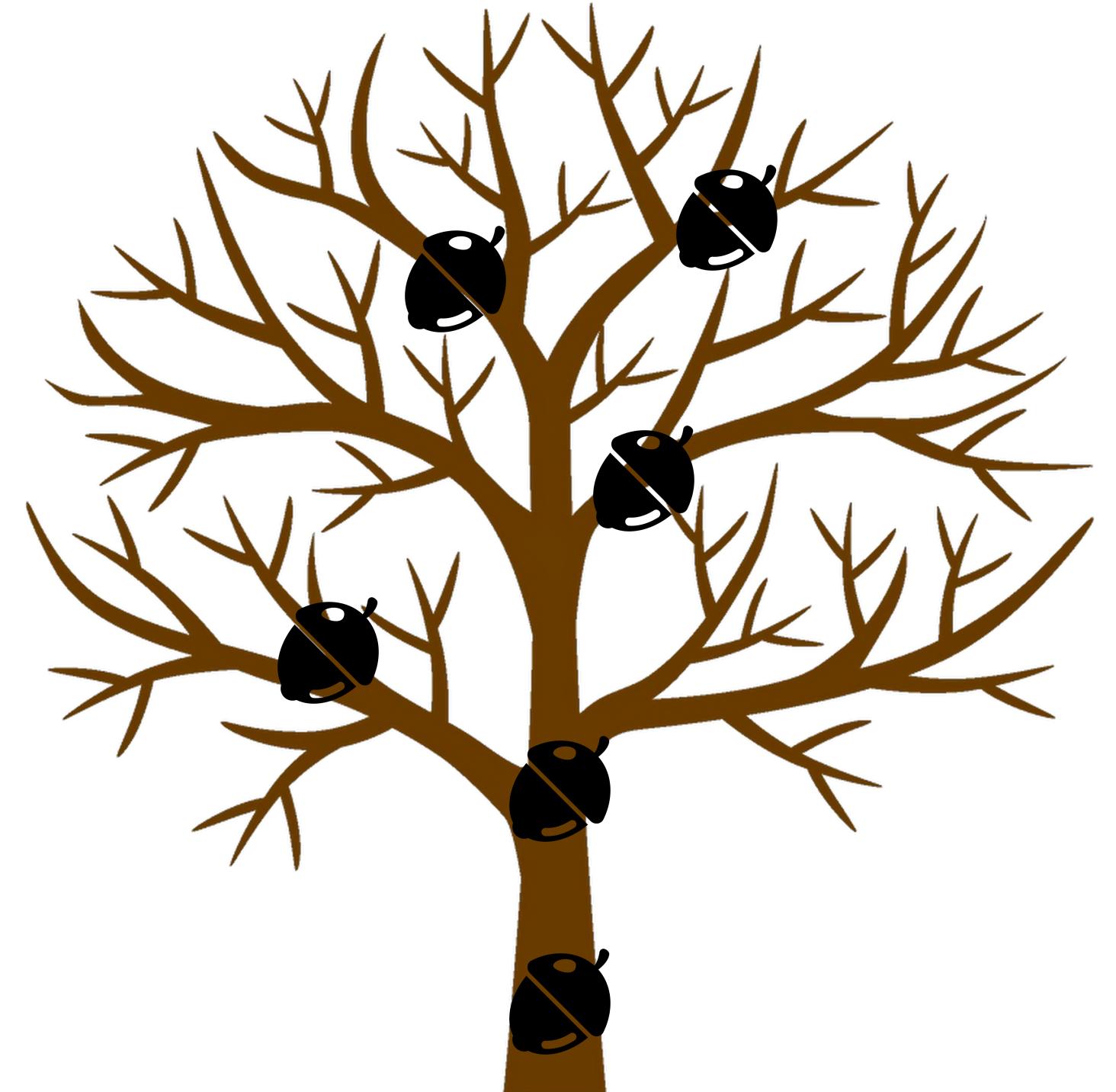
- Each seed represents each step into the program



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

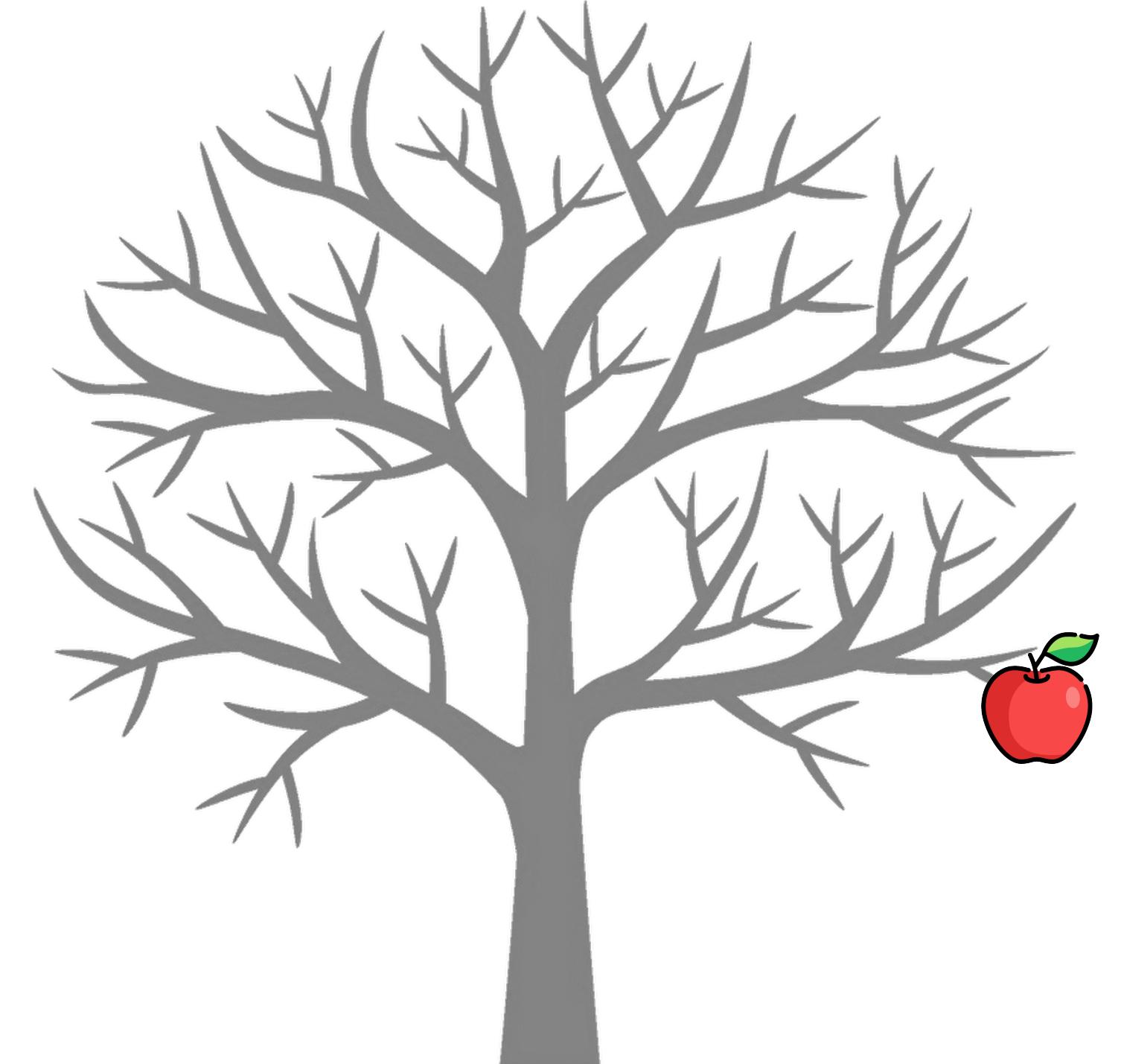
- Each seed represents each step into the program



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

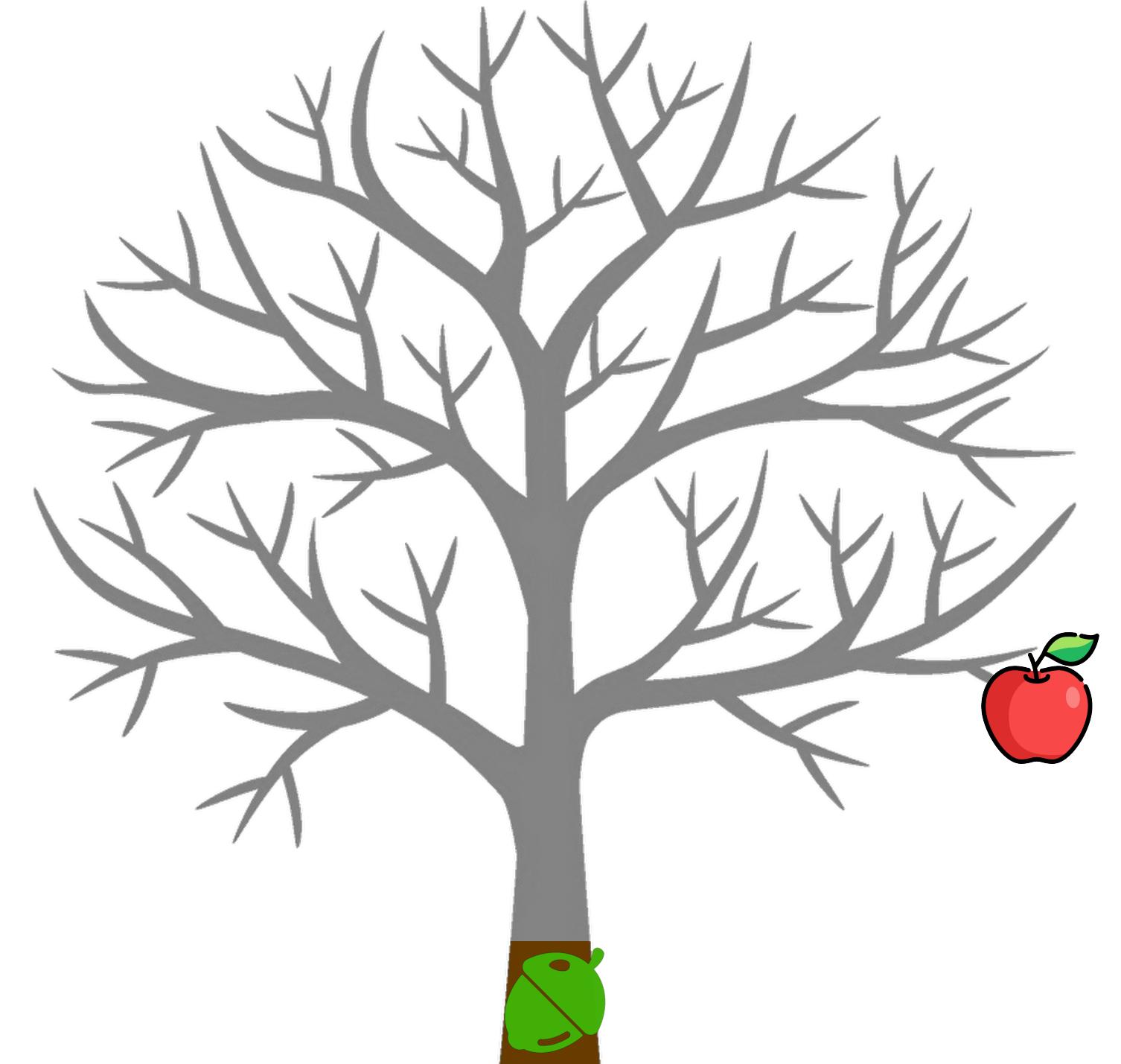
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

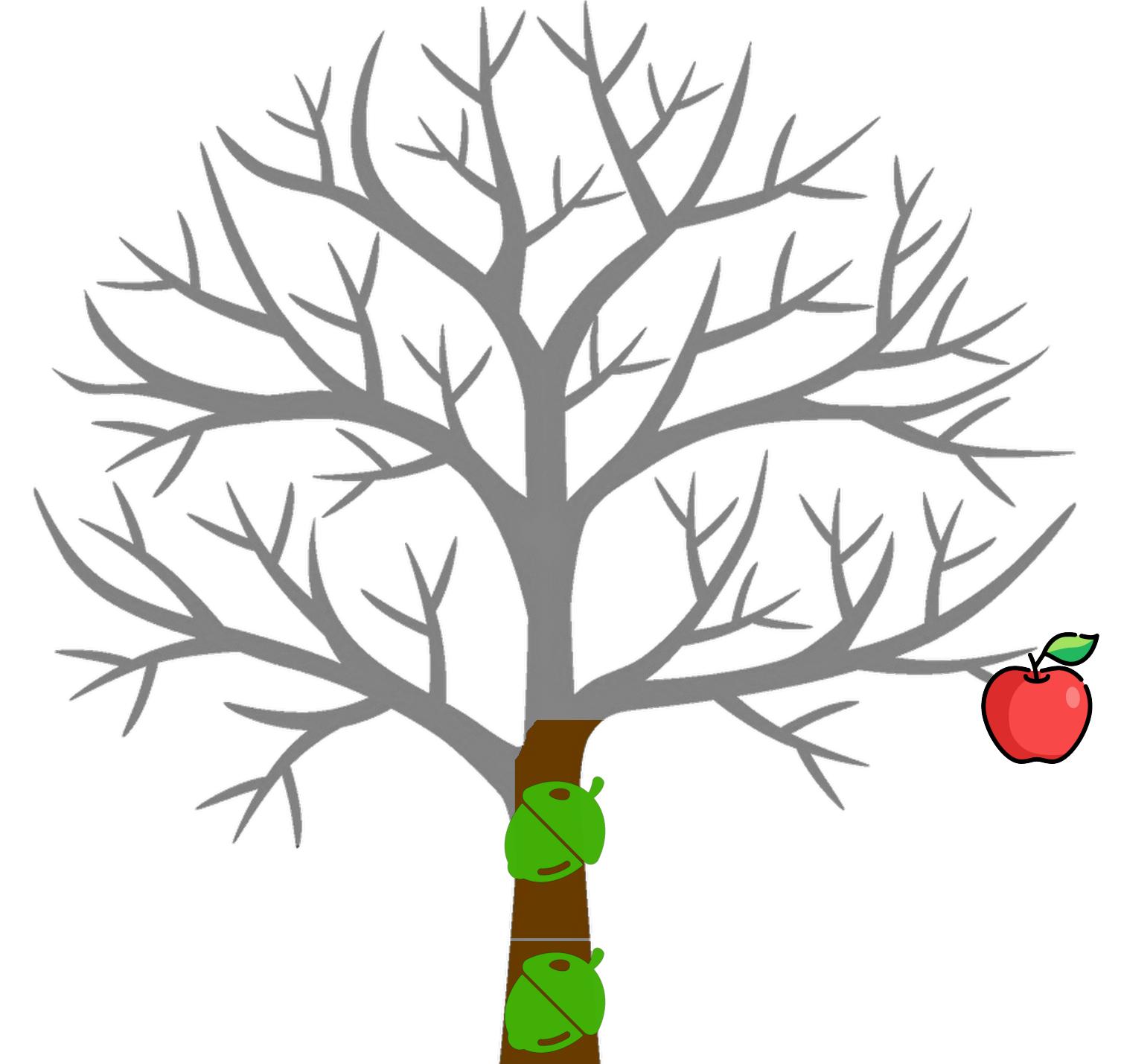
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

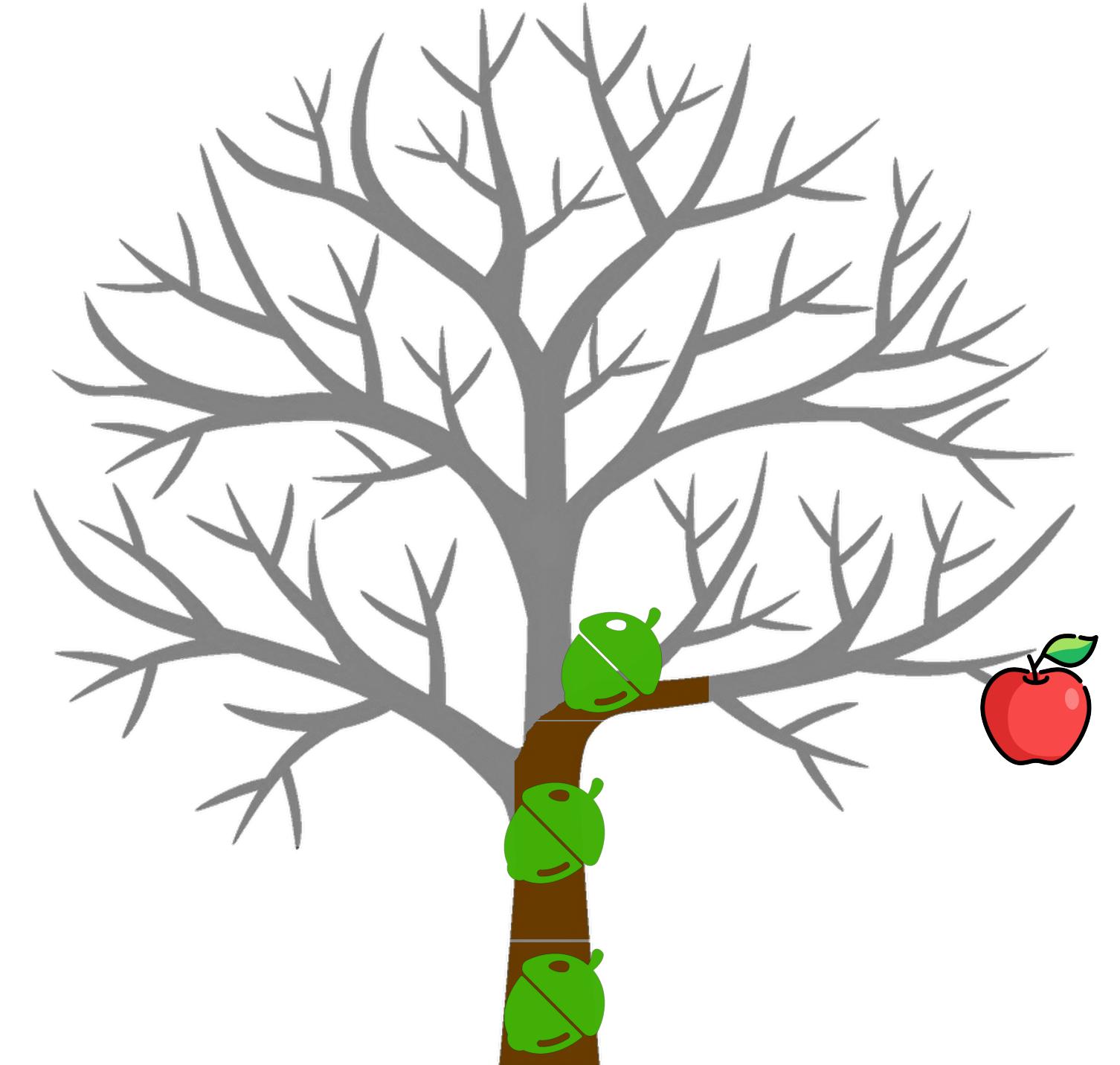
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

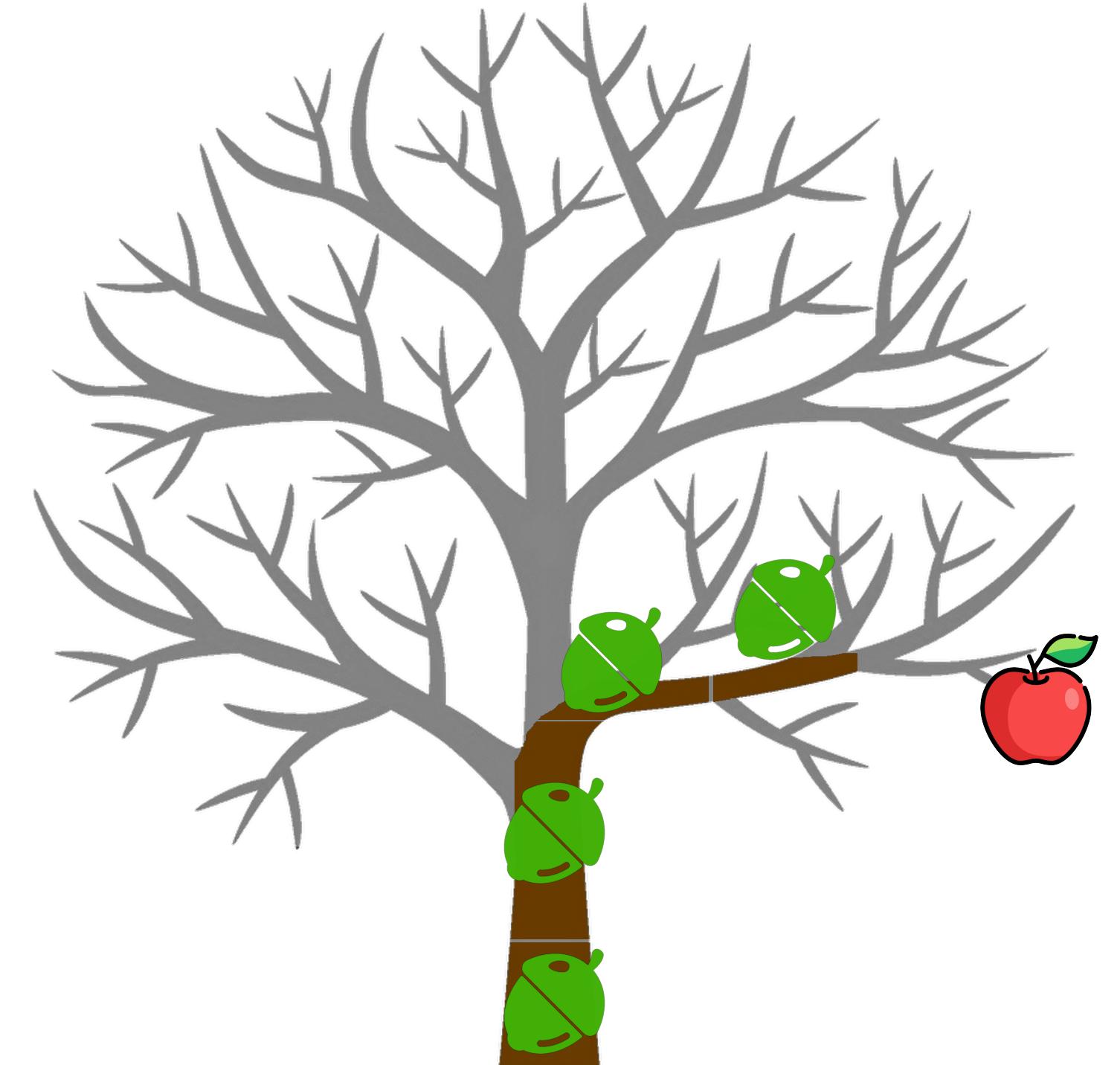
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

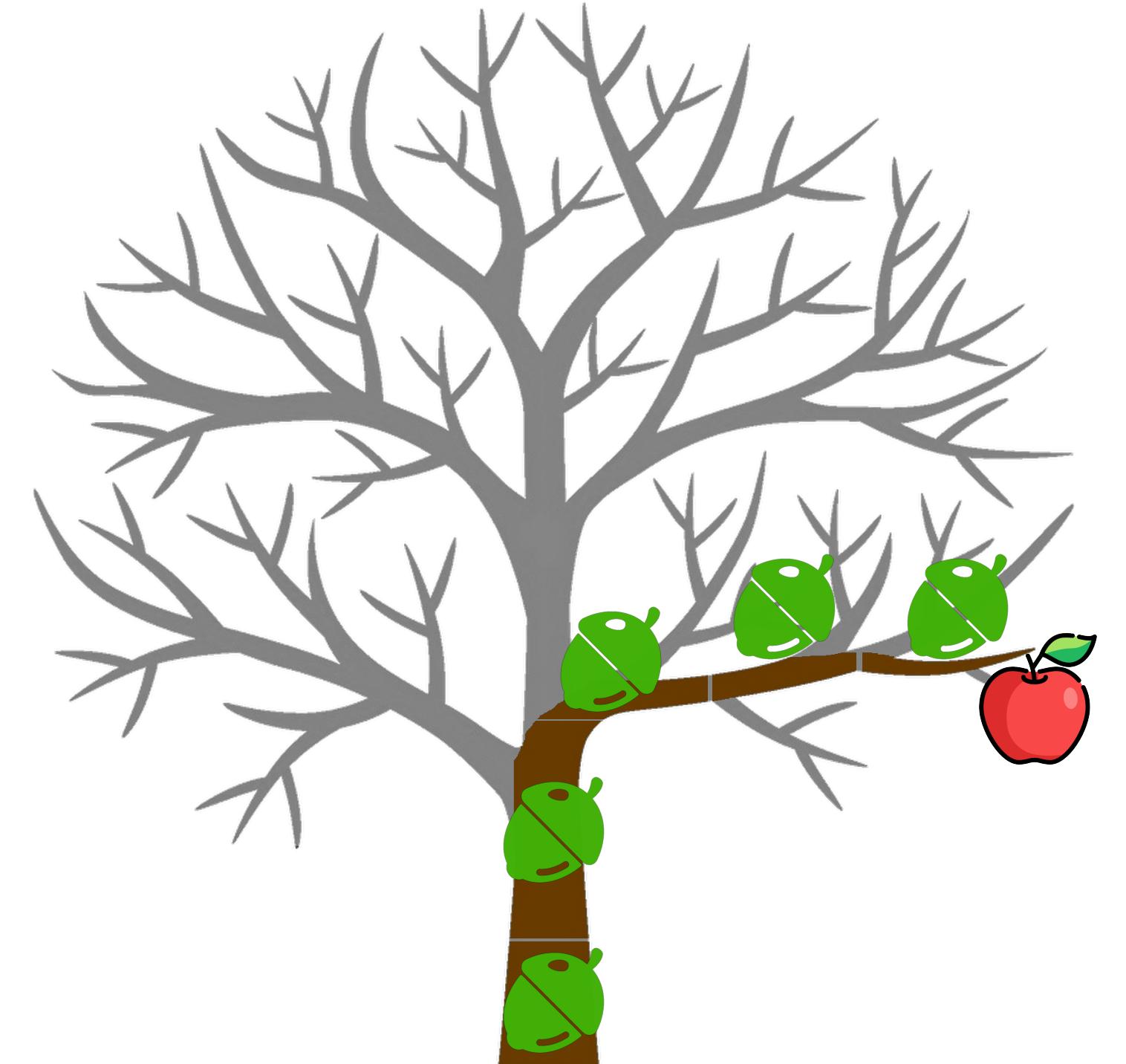
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

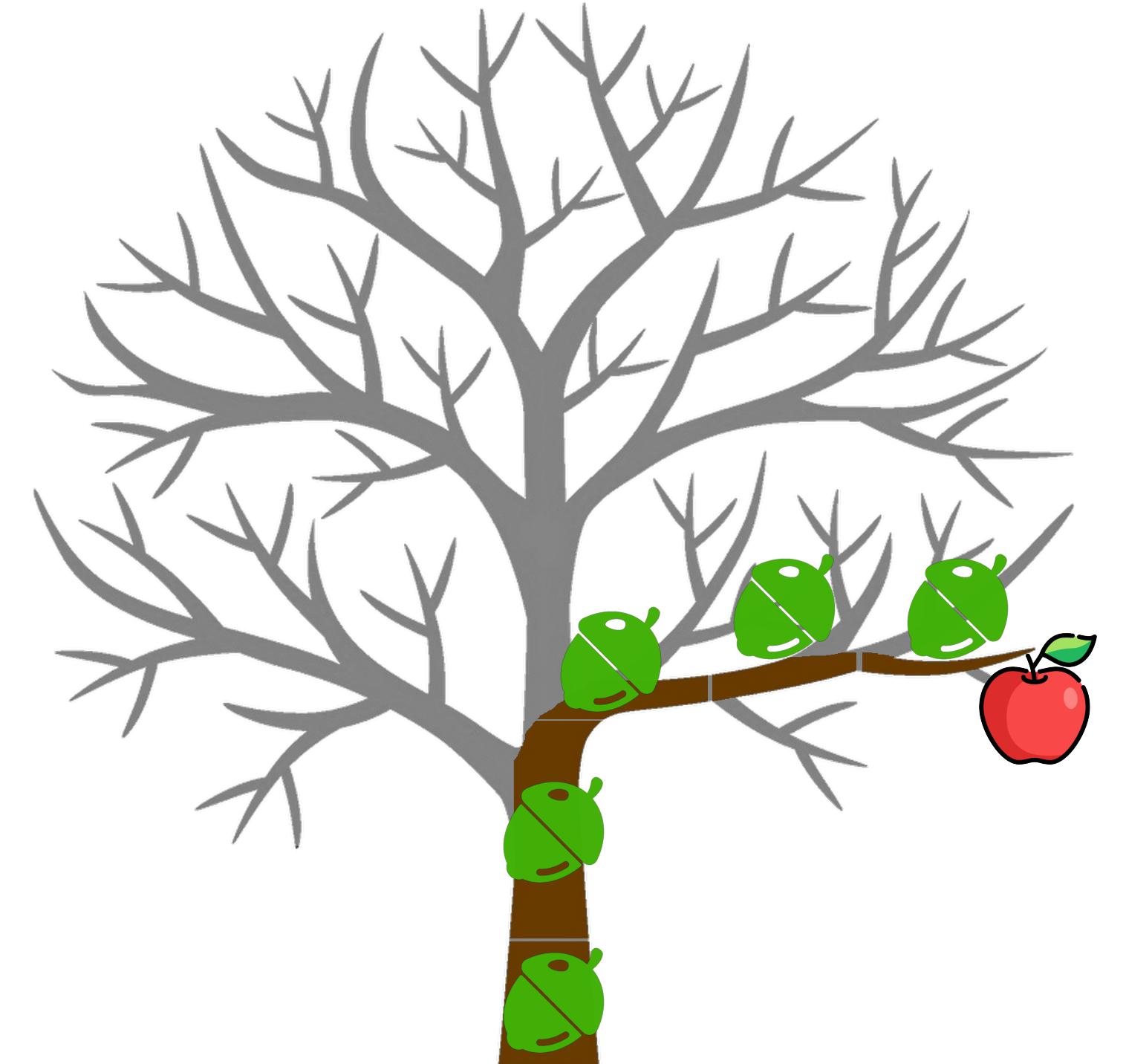
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



# Analysis of Directed Grey-box Fuzzing

## Progress of Fuzzing

- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing
- Understanding the steps of progress is crucial



# Challenge

# Challenge

**Grey-box fuzzer is a black box**

# Challenge

## **Grey-box fuzzer is a black box**

- Too many inputs to keep track of

# Challenge

Number of inputs generated in 24 hours by DAFL<sup>1</sup>

## Grey-box fuzzer is a black box

- Too many inputs to keep track of

Program	All Inputs	Seed Inputs	Crashing Inputs
<b>swftophp</b>	24,727,449	3,839	421
<b>lrzip</b>	4,610,069	676	44
<b>cxxfilt</b>	14,784,726	4,657	346
<b>objcopy</b>	23,562,580	5,207	177
<b>objdump</b>	21,022,357	5,863	175
<b>strip</b>	131,633	1,018	6
<b>nm</b>	5,976,949	2,345	69
<b>readelf</b>	89,493	774	1
<b>xmlint</b>	63,012,643	1,283	2
<b>cjpeg</b>	18,245,672	4,650	20
<b>Average</b>	17,616,357	3,031	126

1. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

# Challenge

Number of inputs generated in 24 hours by DAFL<sup>1</sup>

## Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection

Program	All Inputs	Seed Inputs	Crashing Inputs
<b>swftophp</b>	24,727,449	3,839	421
<b>lrzip</b>	4,610,069	676	44
<b>cxxfilt</b>	14,784,726	4,657	346
<b>objcopy</b>	23,562,580	5,207	177
<b>objdump</b>	21,022,357	5,863	175
<b>strip</b>	131,633	1,018	6
<b>nm</b>	5,976,949	2,345	69
<b>readelf</b>	89,493	774	1
<b>xmlint</b>	63,012,643	1,283	2
<b>cjpeg</b>	18,245,672	4,650	20
<b>Average</b>	17,616,357	3,031	126

1. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

# Challenge

Number of inputs generated in 24 hours by DAFL<sup>1</sup>

## Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

Program	All Inputs	Seed Inputs	Crashing Inputs
<b>swftophp</b>	24,727,449	3,839	421
<b>lrzip</b>	4,610,069	676	44
<b>cxxfilt</b>	14,784,726	4,657	346
<b>objcopy</b>	23,562,580	5,207	177
<b>objdump</b>	21,022,357	5,863	175
<b>strip</b>	131,633	1,018	6
<b>nm</b>	5,976,949	2,345	69
<b>readelf</b>	89,493	774	1
<b>xmllint</b>	63,012,643	1,283	2
<b>cjpeg</b>	18,245,672	4,650	20
<b>Average</b>	17,616,357	3,031	126

1. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

# Challenge

## **Grey-box fuzzer is a black box**

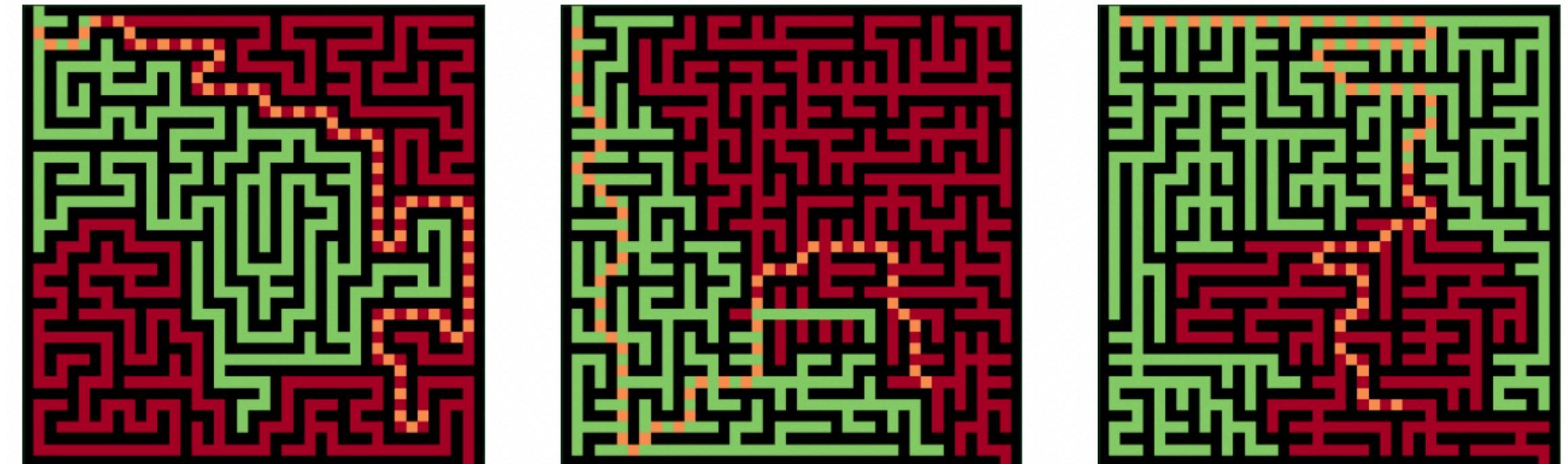
- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

## **Visualization Tools**

# Challenge

## Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance



Visualization of Fuzzle<sup>1</sup>

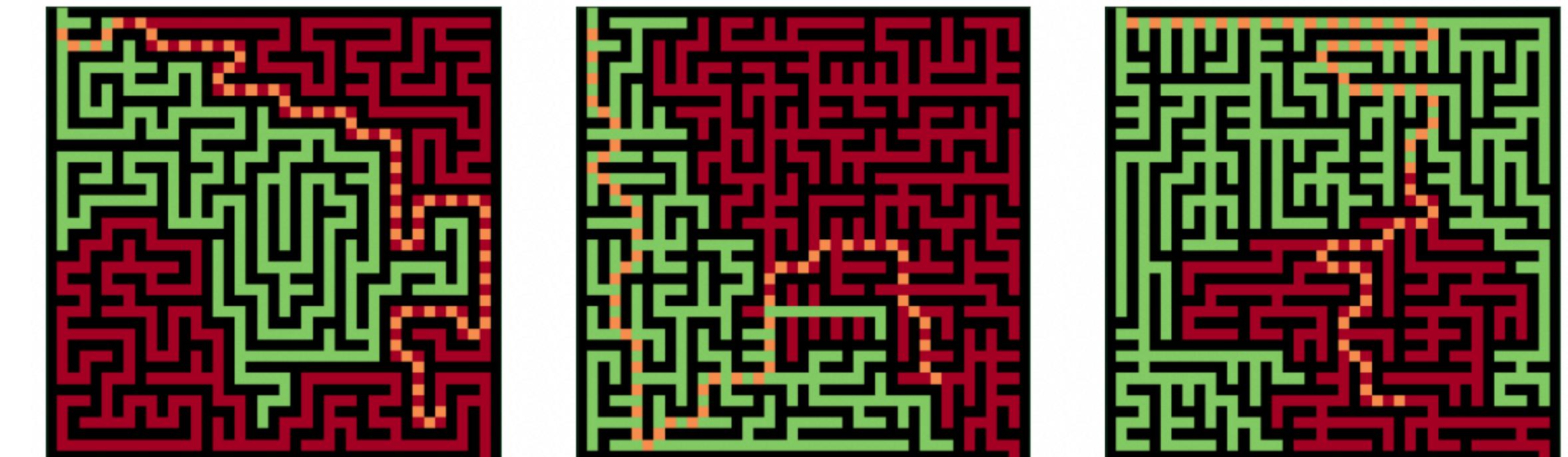
## Visualization Tools

1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022

# Challenge

## Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance



Visualization of Fuzzle<sup>1</sup>

## Visualization Tools

LCOV - code coverage report		
Current view: top level		
Test: id:002084,src:002034,op:havoc,rep:2.lcov_info_final	Lines:	Hit Total Coverage
Date: 2015-05-25	Functions:	3270 7970 41.0 %
	Branches:	224 390 57.4 %
		1778 5269 33.7 %

Directory	Line Coverage	Functions	Branches
server	28.4 %	876 / 3080	39.5 % 49 / 124 27.0 % 541 / 2007
client	33.8 %	690 / 2039	54.9 % 39 / 71 31.5 % 397 / 1260
lib	59.8 %	1704 / 2851	69.7 % 136 / 195 42.0 % 840 / 2002

Generated by: [LCOV version 1.10](#)

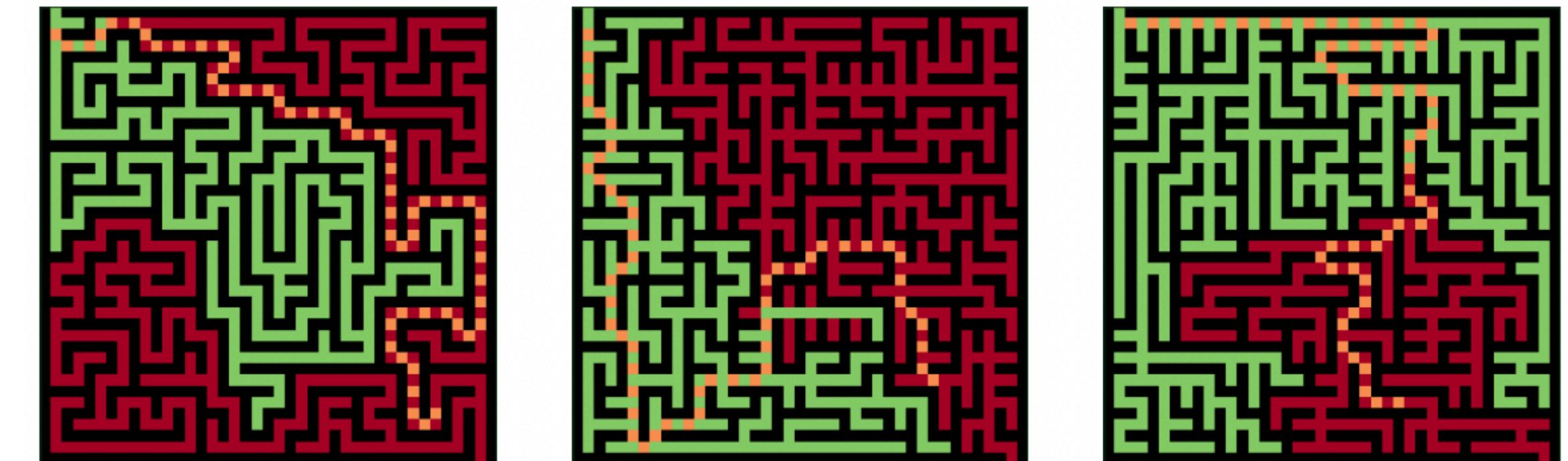
Visualization of afl-cov<sup>2</sup>

1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022
2. "afl-cov - AFL Fuzzing Code Coverage", Rash

# Challenge

## Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance



Visualization of Fuzzle<sup>1</sup>

LCOV - code coverage report		
Current view: top level		
Test: id:002084,src:002034,op:havoc,rep:2.lcov_info_final	Lines:	Hit Total Coverage
Date: 2015-05-25	Functions:	3270 7970 41.0 %
	Branches:	224 390 57.4 %
		1778 5269 33.7 %

Directory	Line Coverage	Functions	Branches
server	28.4 %	876 / 3080	39.5 % 49 / 124 27.0 % 541 / 2007
client	33.8 %	690 / 2039	54.9 % 39 / 71 31.5 % 397 / 1260
lib	59.8 %	1704 / 2851	69.7 % 136 / 195 42.0 % 840 / 2002

Generated by: [LCOV version 1.10](#)

## Visualization Tools

- Focused on coverage analysis

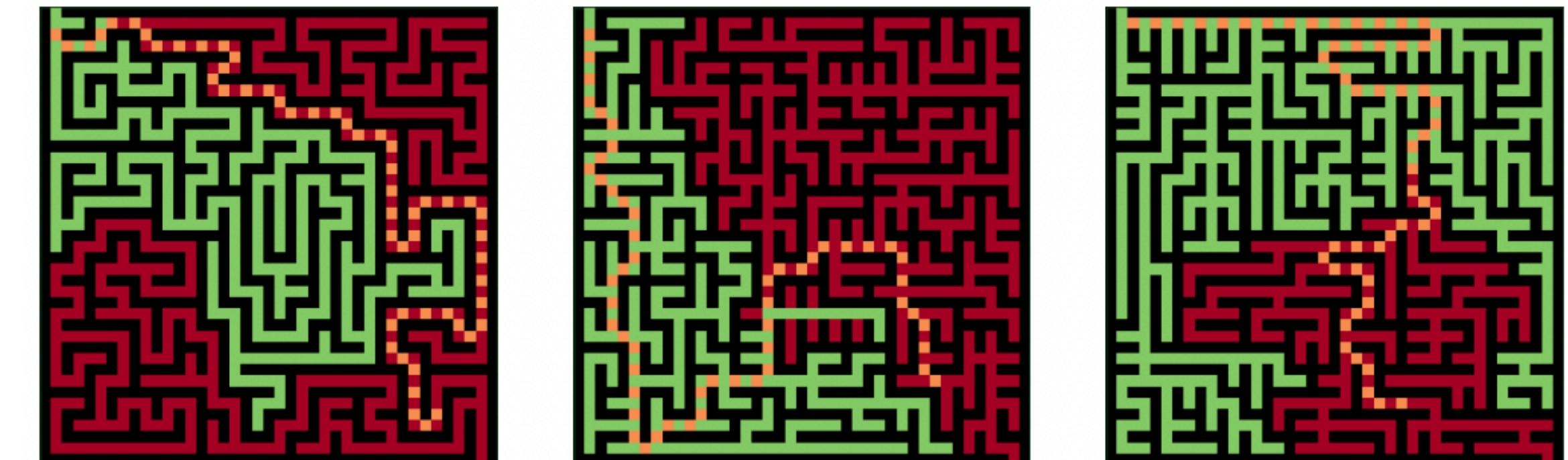
Visualization of afl-cov<sup>2</sup>

1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022
2. "afl-cov - AFL Fuzzing Code Coverage", Rash

# Challenge

## Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance



Visualization of Fuzzle<sup>1</sup>

## Visualization Tools

- Focused on coverage analysis
- Insufficient for directed setting

LCOV - code coverage report		
Current view: top level		
Test: id:002084,src:002034,op:havoc,rep:2.lcov_info_final	Lines:	Hit Total Coverage
Date: 2015-05-25	2370 7970	41.0 %
	Functions:	224 390 57.4 %
	Branches:	1778 5269 33.7 %

Directory	Line Coverage	Functions	Branches
server	28.4 %	876 / 3080	39.5 % 49 / 124 27.0 % 541 / 2007
client	33.8 %	690 / 2039	54.9 % 39 / 71 31.5 % 397 / 1260
lib	59.8 %	1704 / 2851	69.7 % 136 / 195 42.0 % 840 / 2002

Generated by: [LCOV version 1.10](#)

Visualization of afl-cov<sup>2</sup>

1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022
2. "afl-cov - AFL Fuzzing Code Coverage", Rash

# Our Solution

# Our Solution

**GeneVis: Genealogical Visualization Tool**

# Our Solution

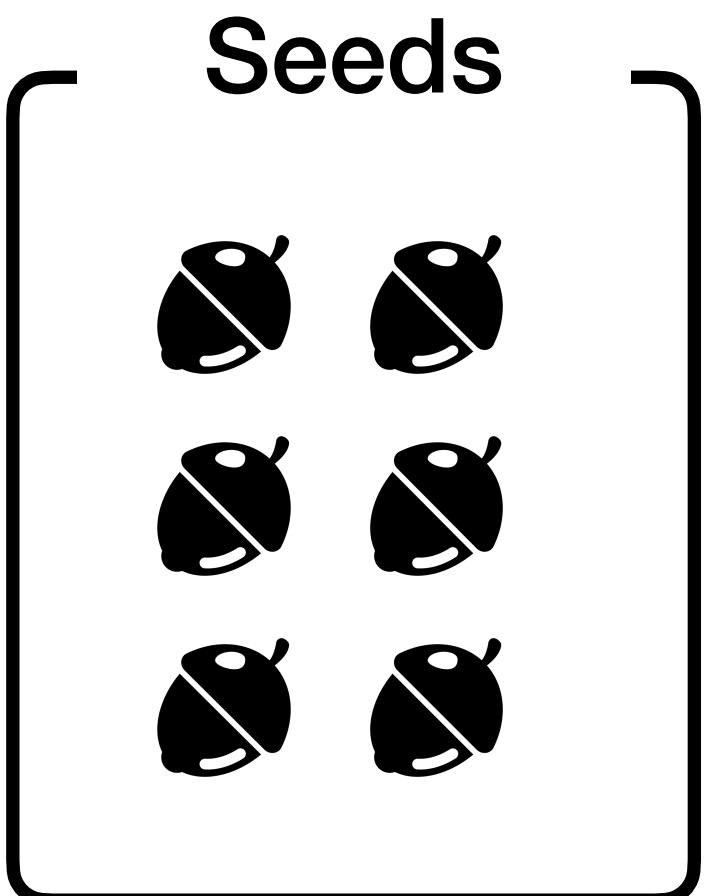
## **GeneVis: Genealogical Visualization Tool**

- Tree structure based on the relationship between inputs

# Our Solution

## GeneVis: Genealogical Visualization Tool

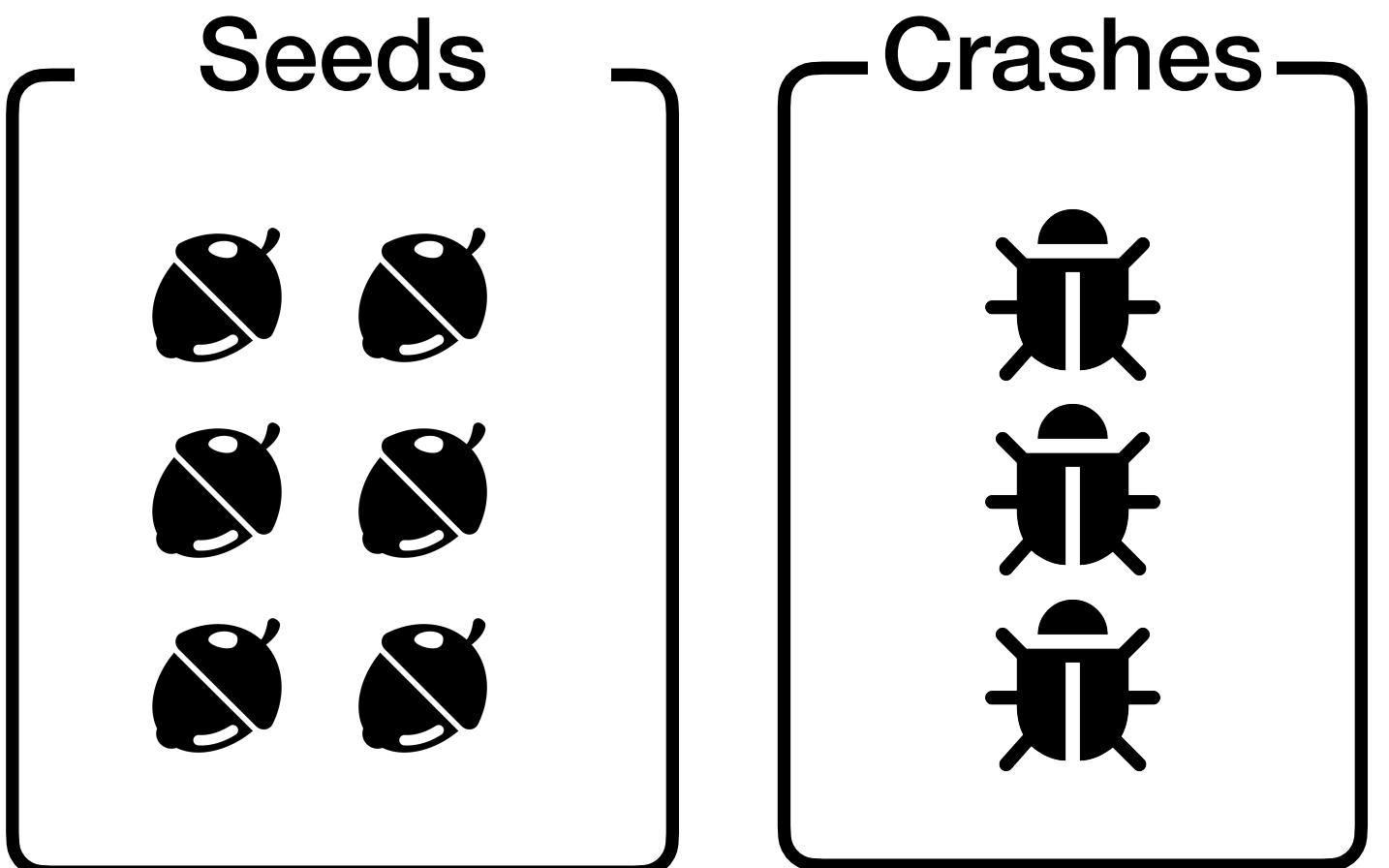
- Tree structure based on the relationship between inputs



# Our Solution

## GeneVis: Genealogical Visualization Tool

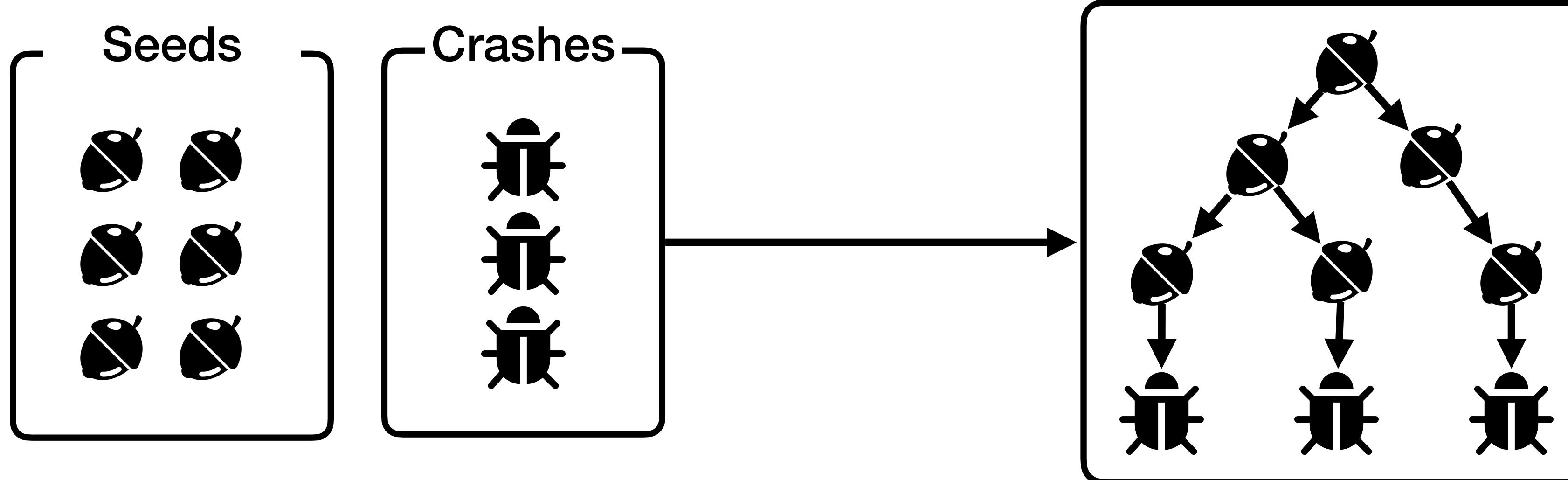
- Tree structure based on the relationship between inputs



# Our Solution

## GeneVis: Genealogical Visualization Tool

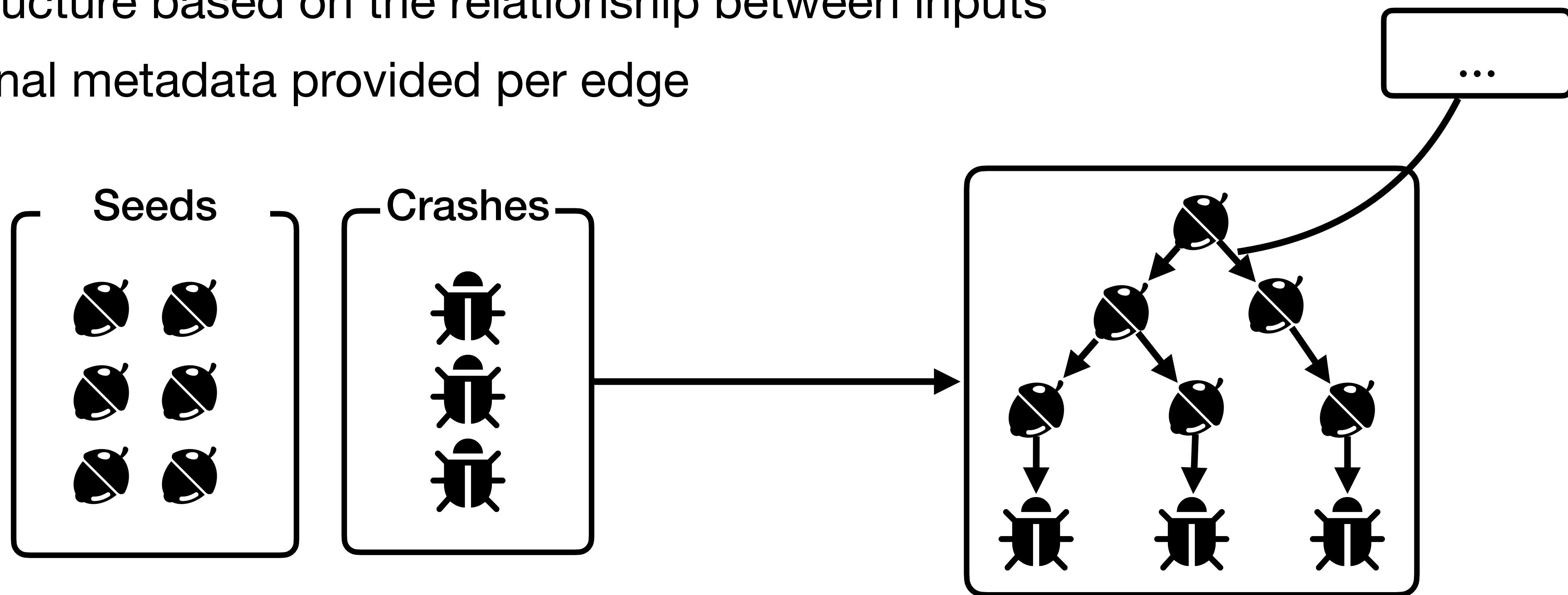
- Tree structure based on the relationship between inputs



# Our Solution

## GeneVis: Genealogical Visualization Tool

- Tree structure based on the relationship between inputs
- Additional metadata provided per edge



# Overview

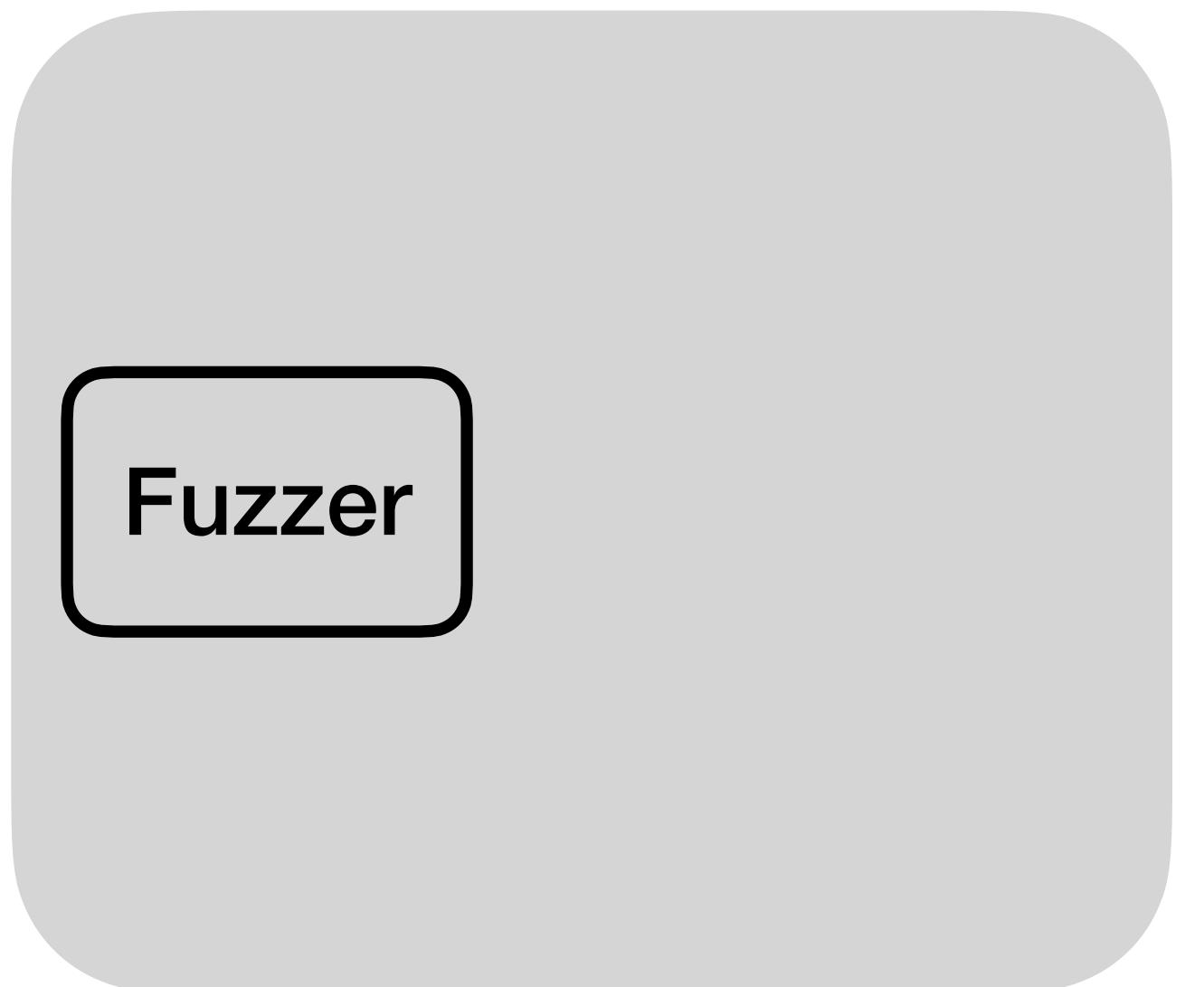
# Overview

## Fuzzing Phase



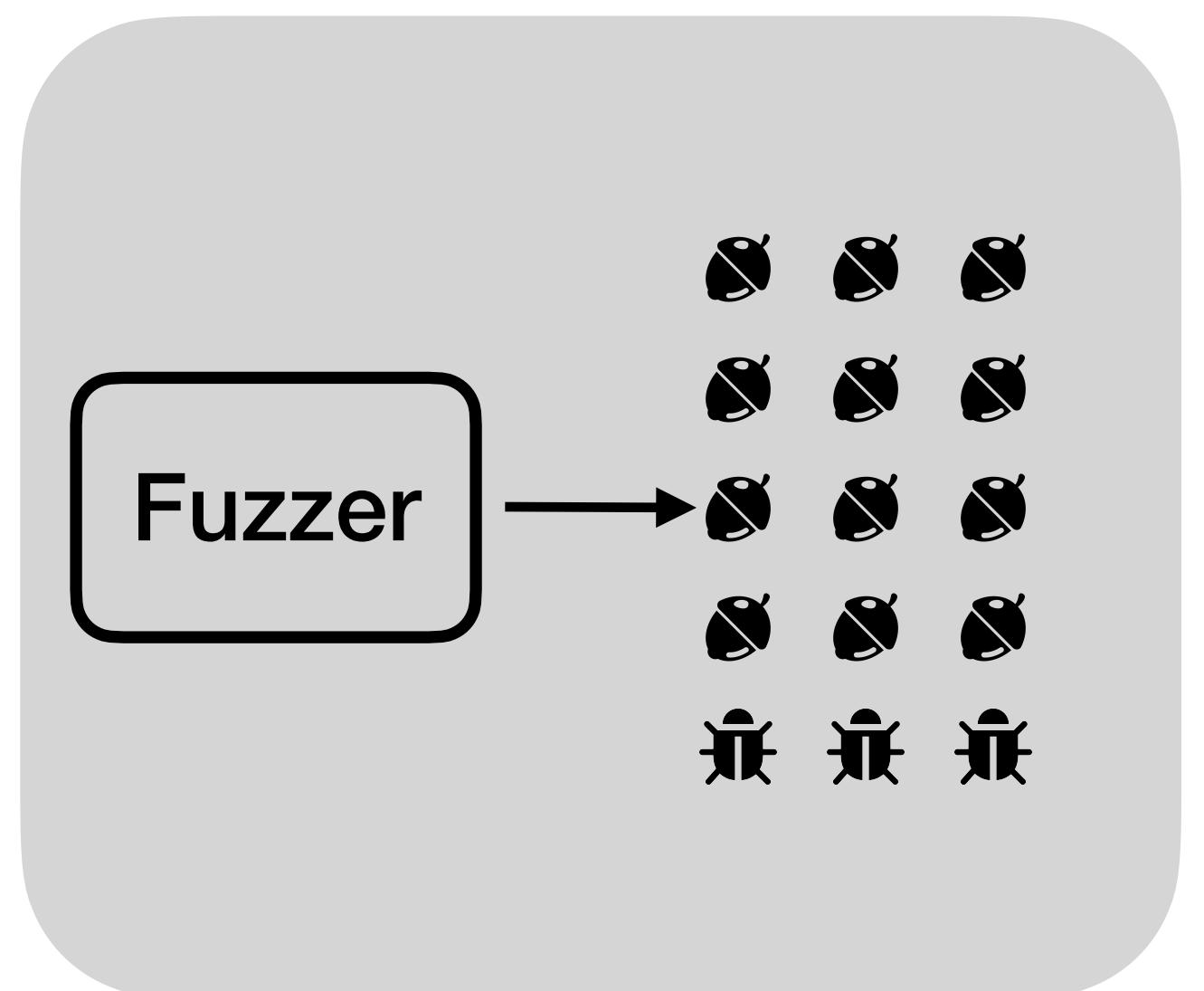
# Overview

## Fuzzing Phase



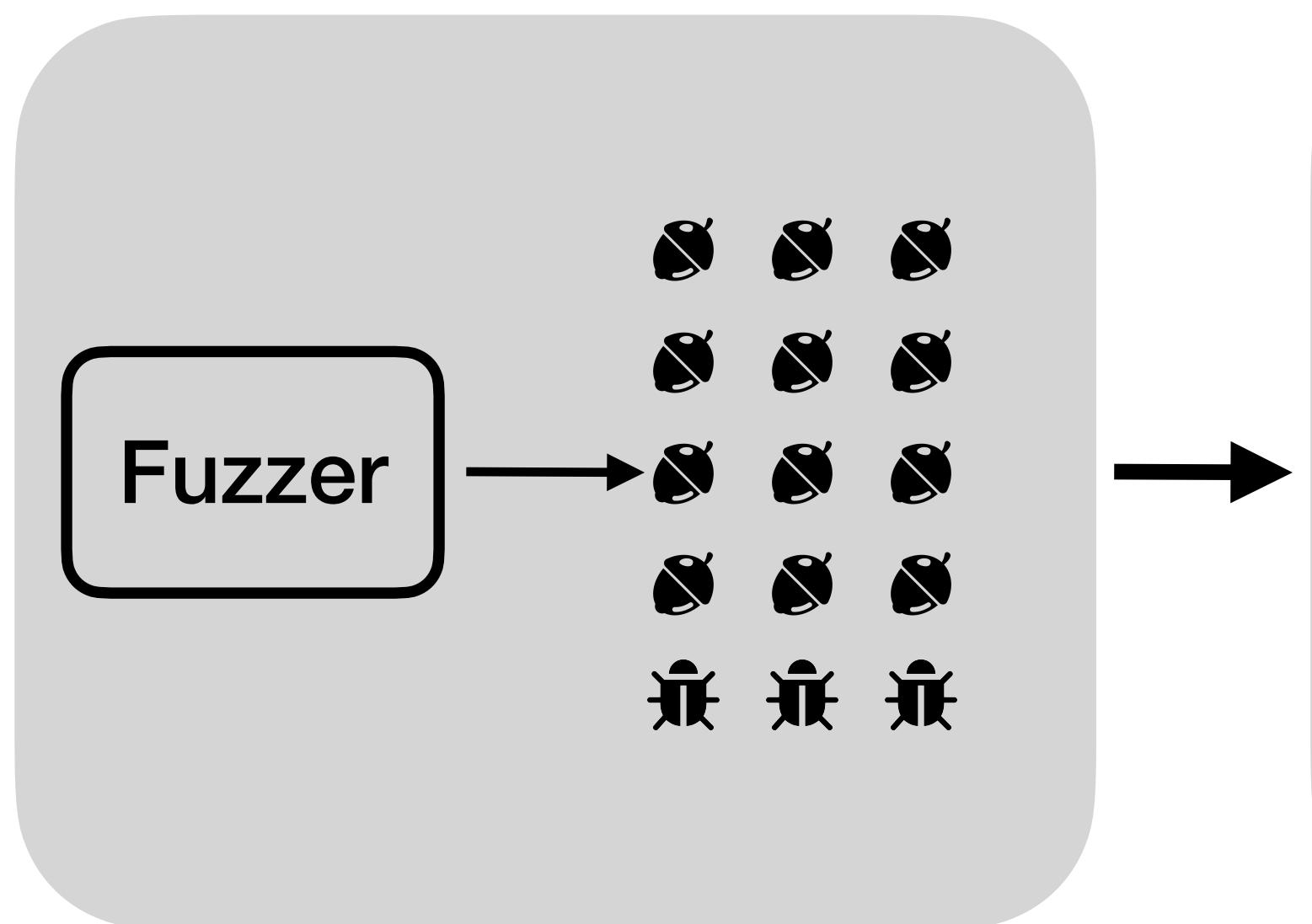
# Overview

## Fuzzing Phase



# Overview

Fuzzing Phase

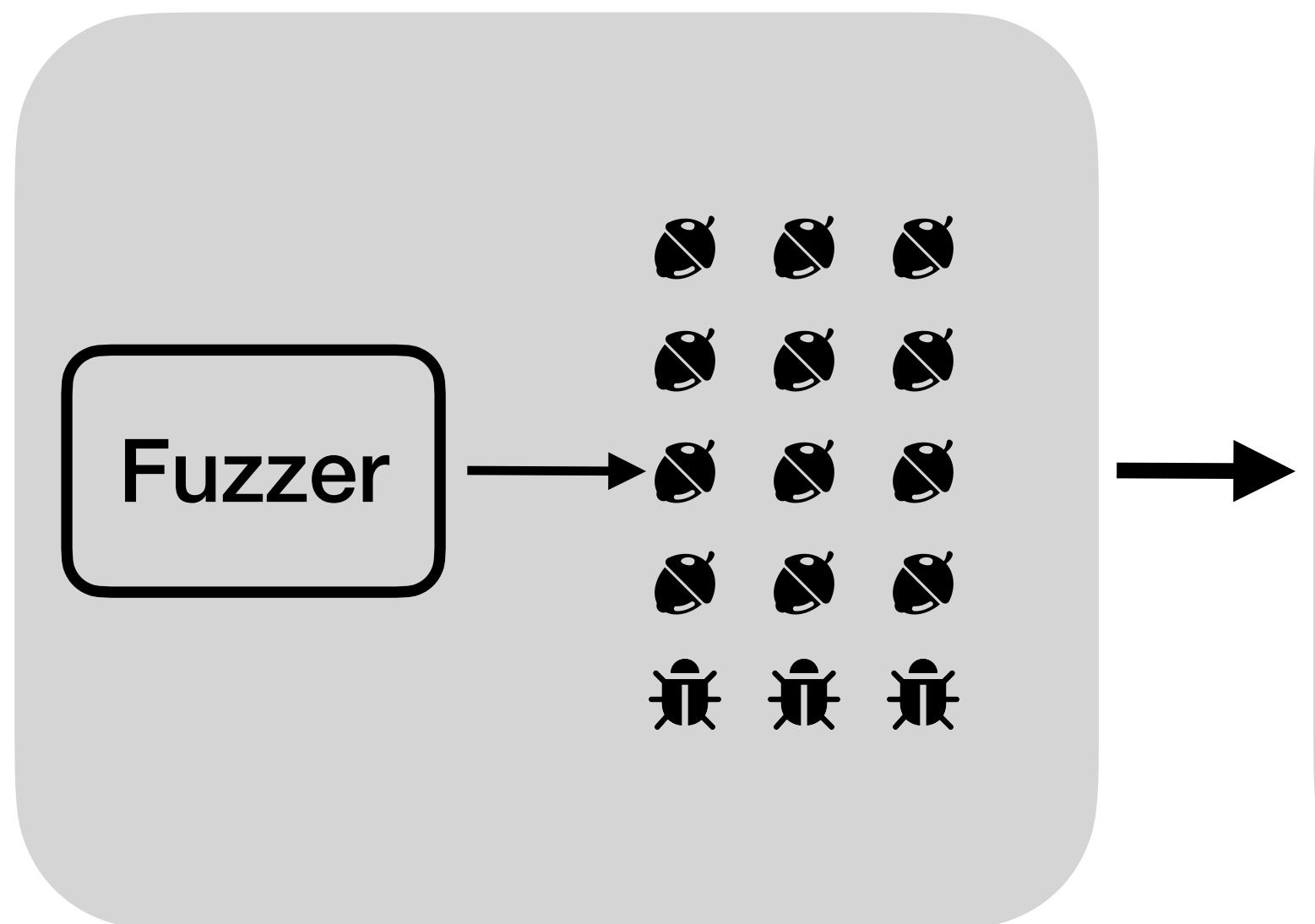


Data Collection Phase

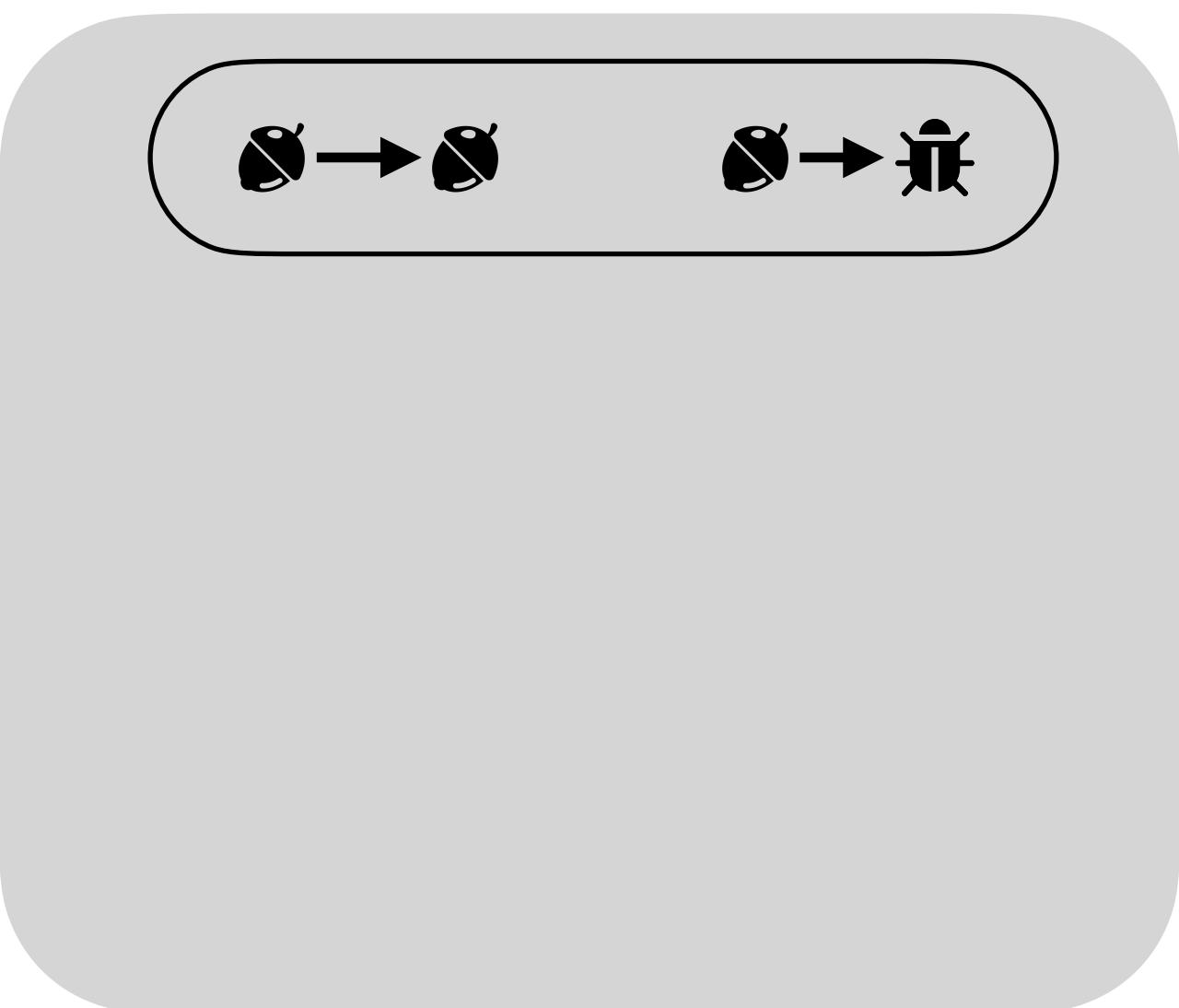


# Overview

Fuzzing Phase

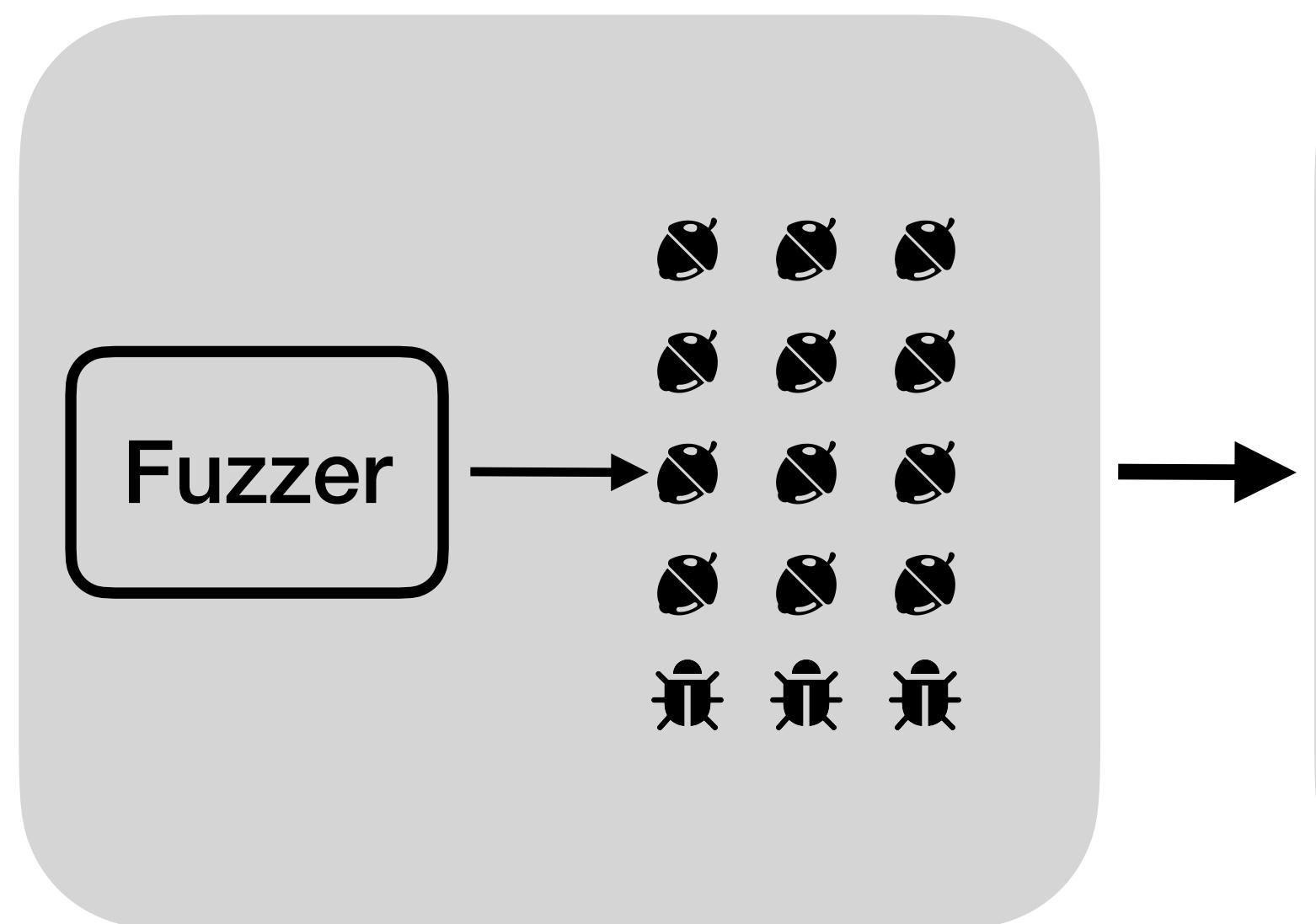


Data Collection Phase

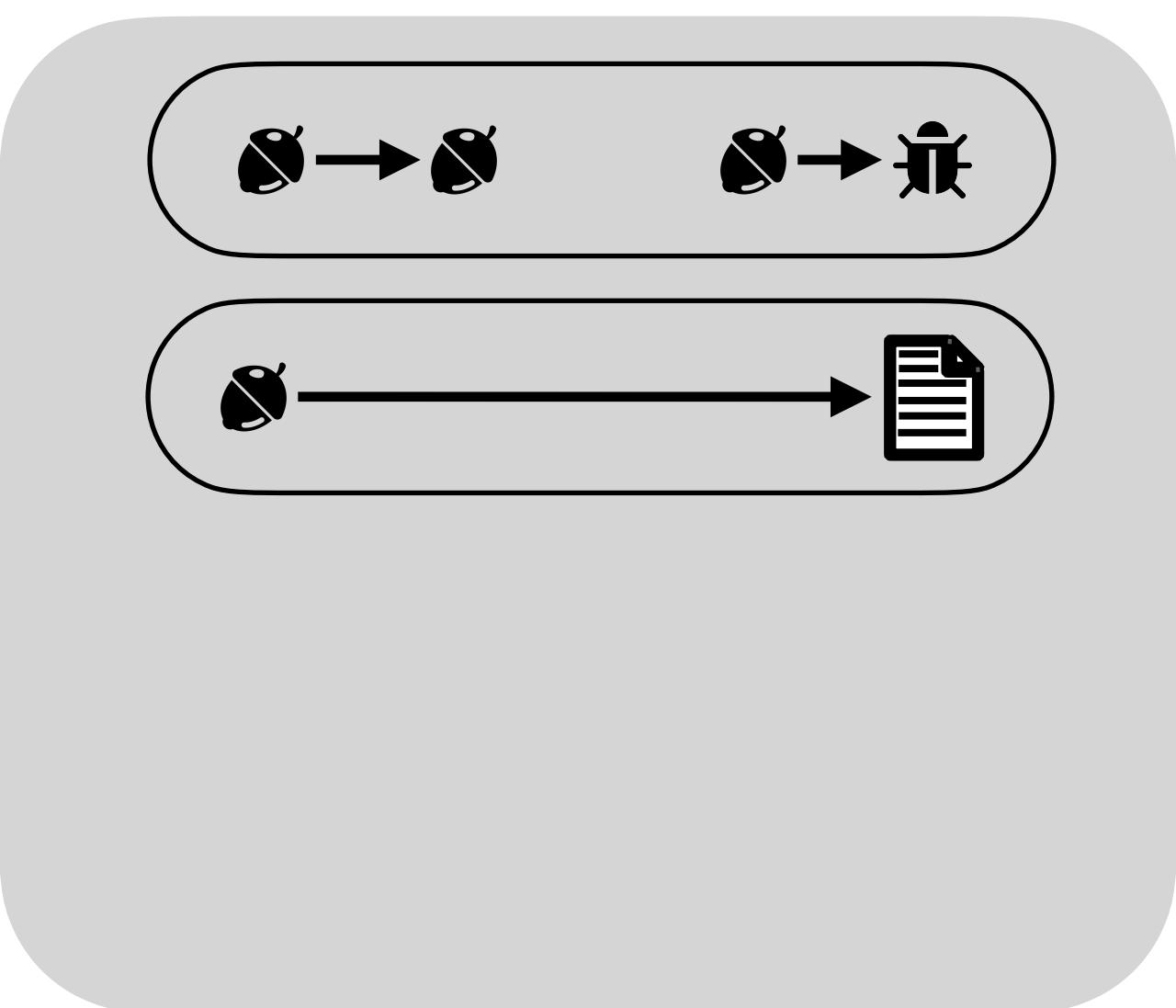


# Overview

## Fuzzing Phase

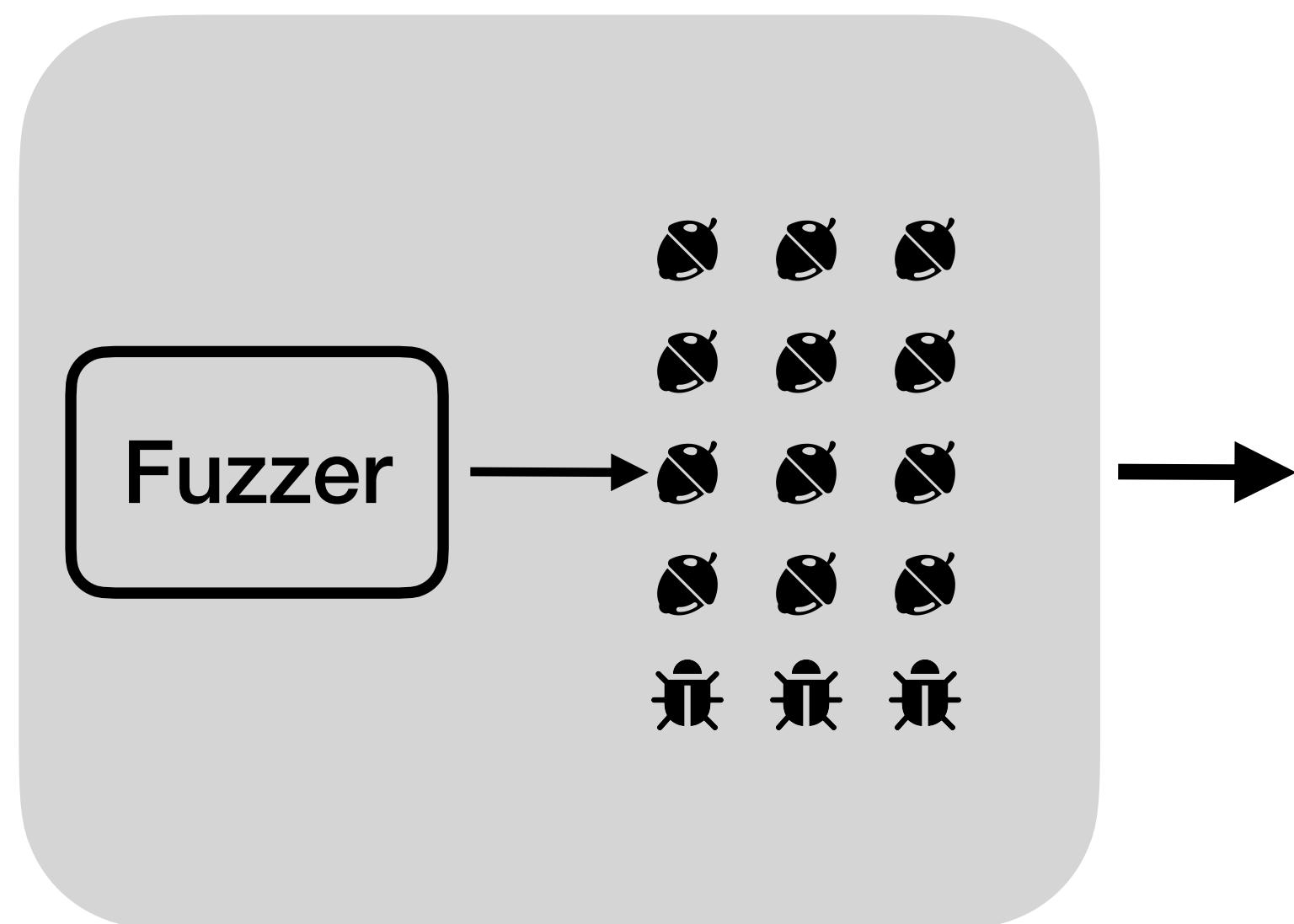


## Data Collection Phase

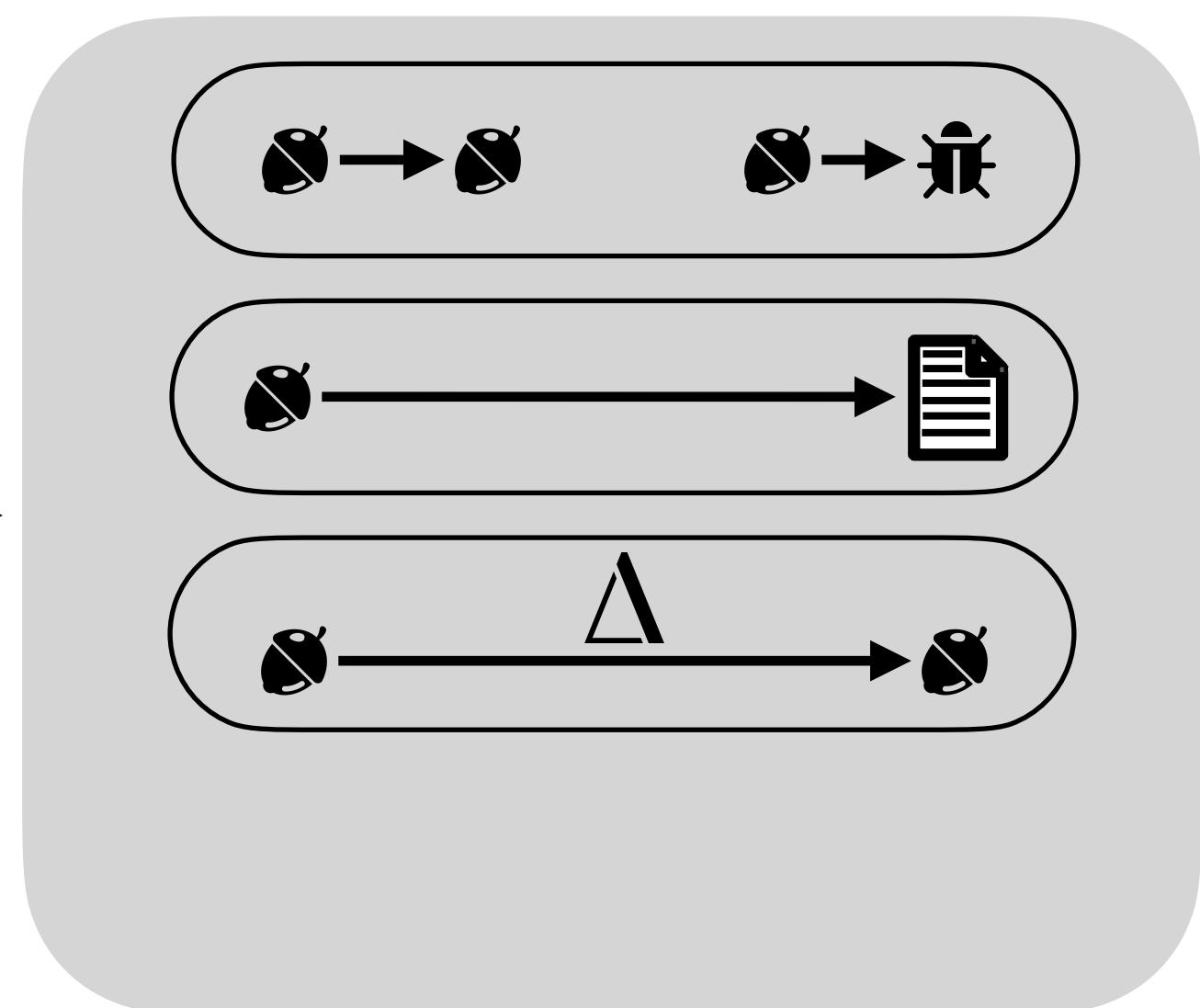


# Overview

## Fuzzing Phase

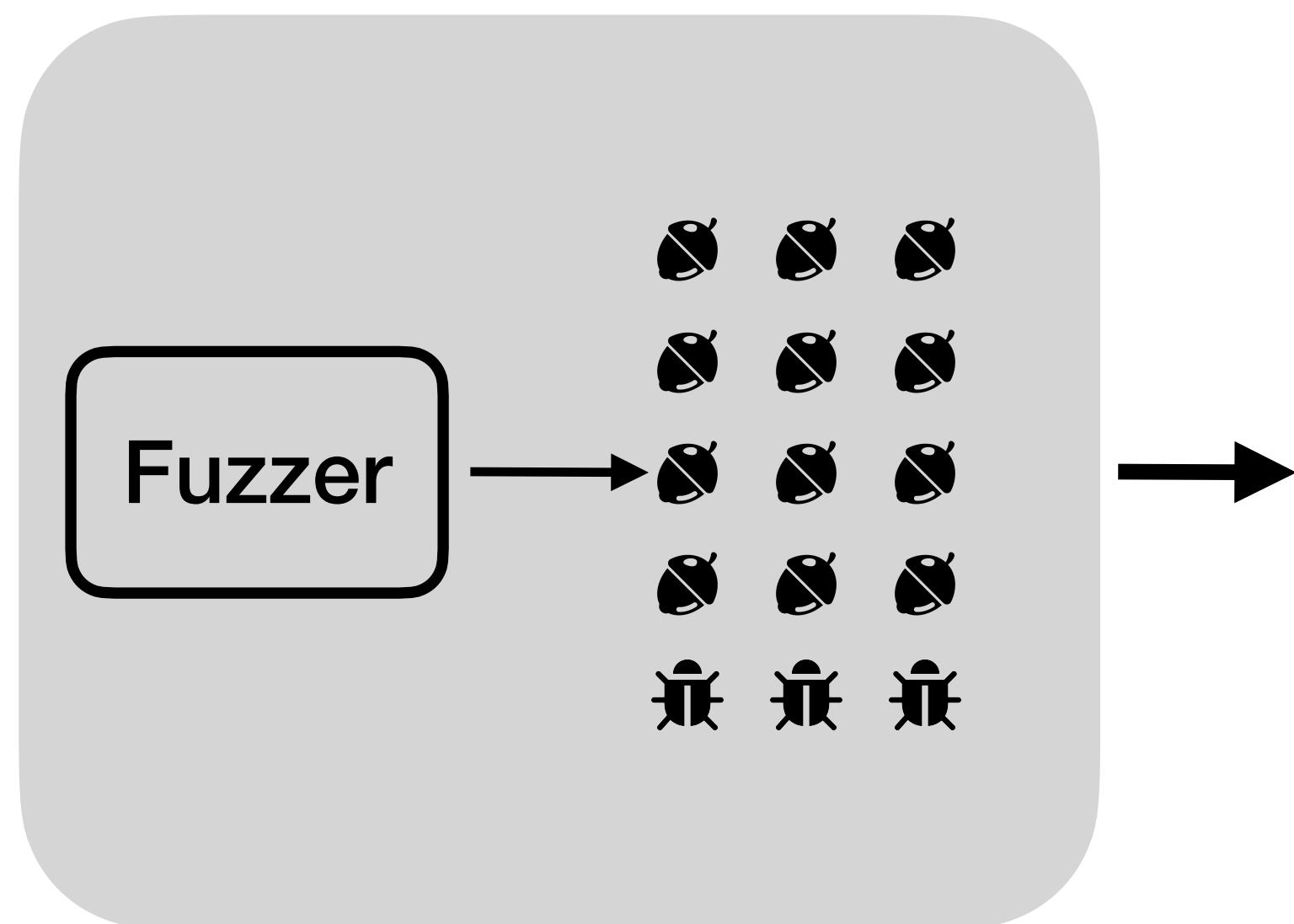


## Data Collection Phase

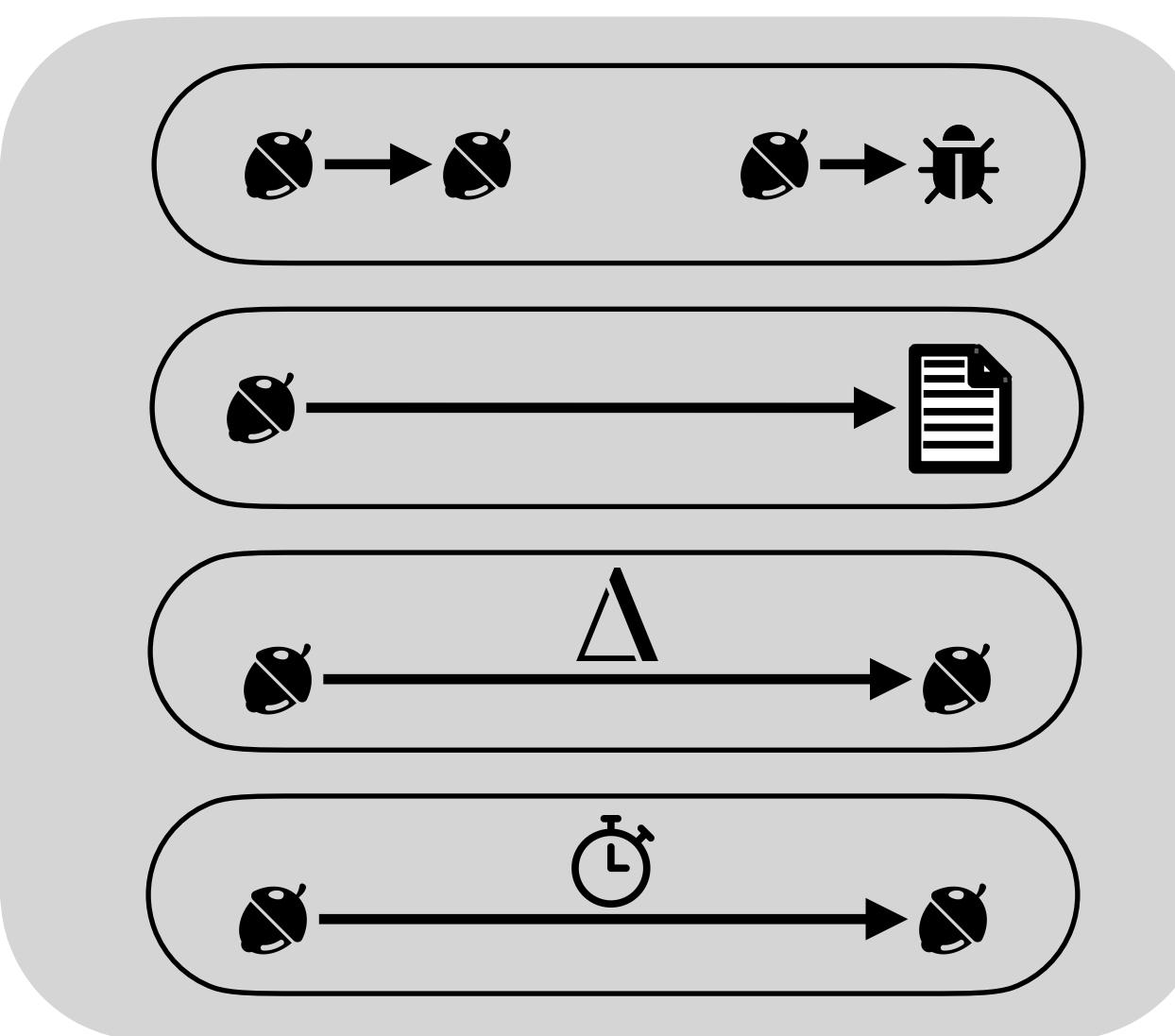


# Overview

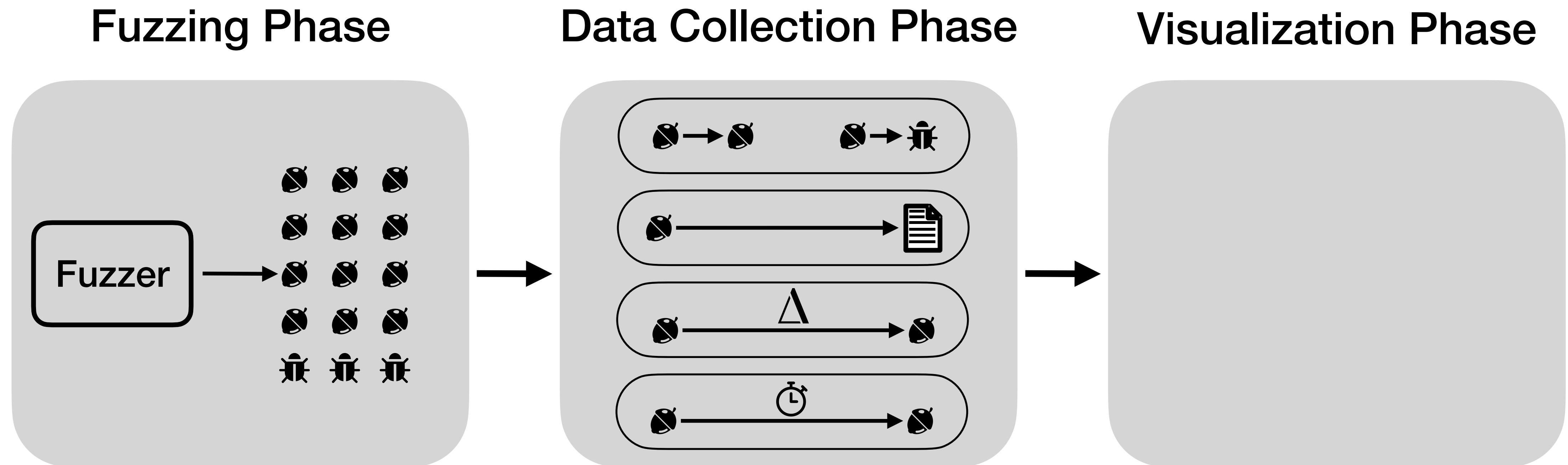
## Fuzzing Phase



## Data Collection Phase

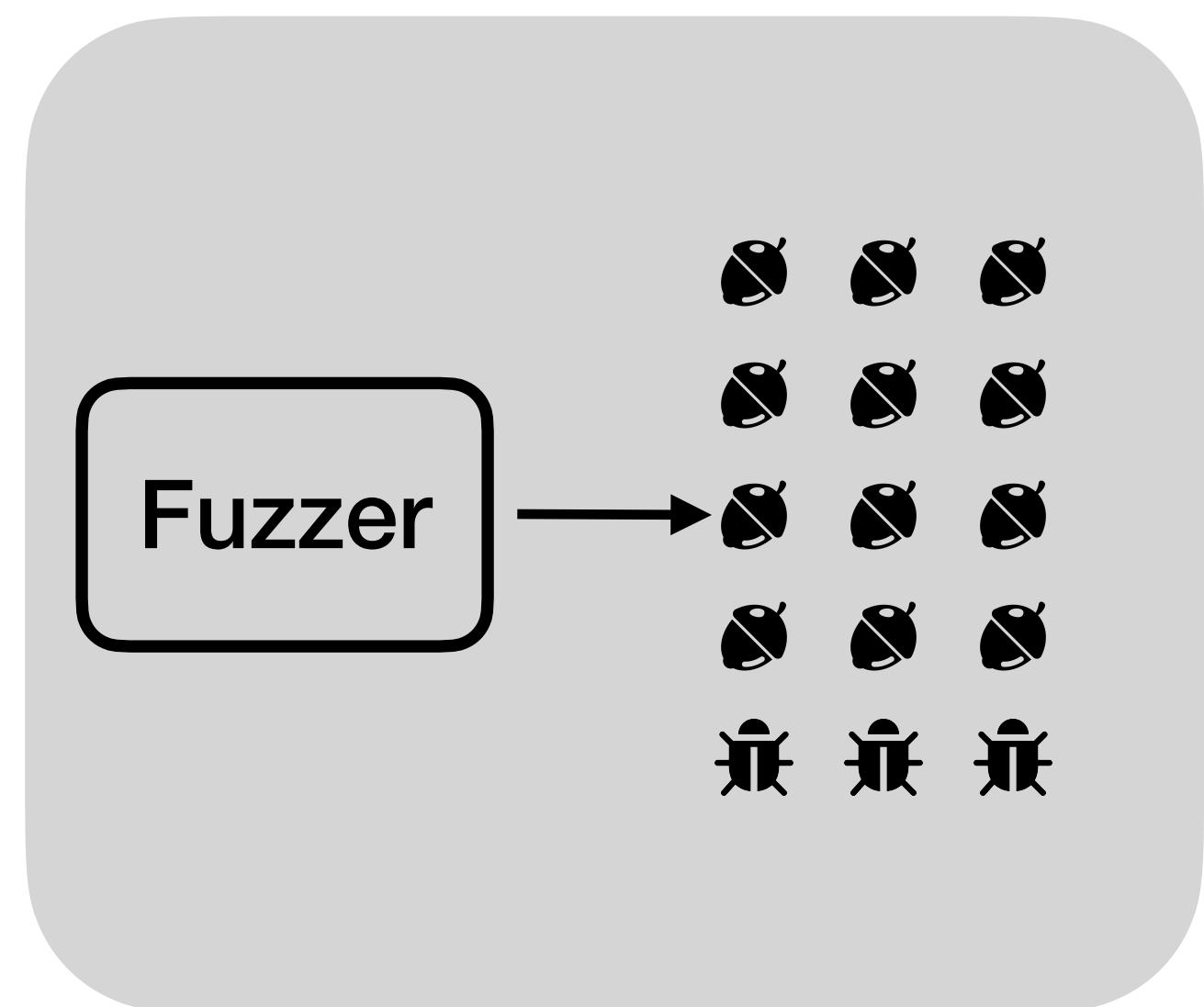


# Overview

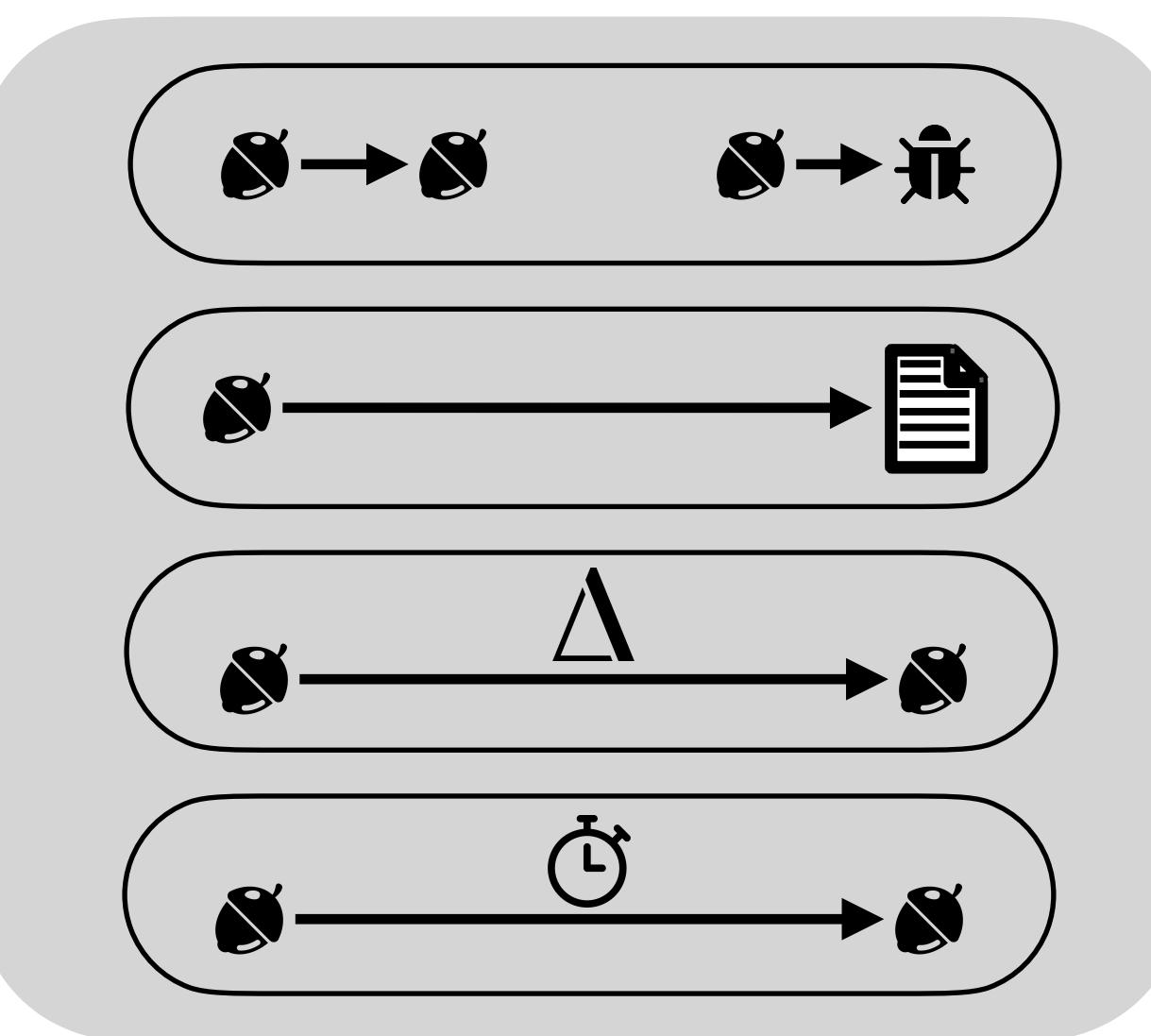


# Overview

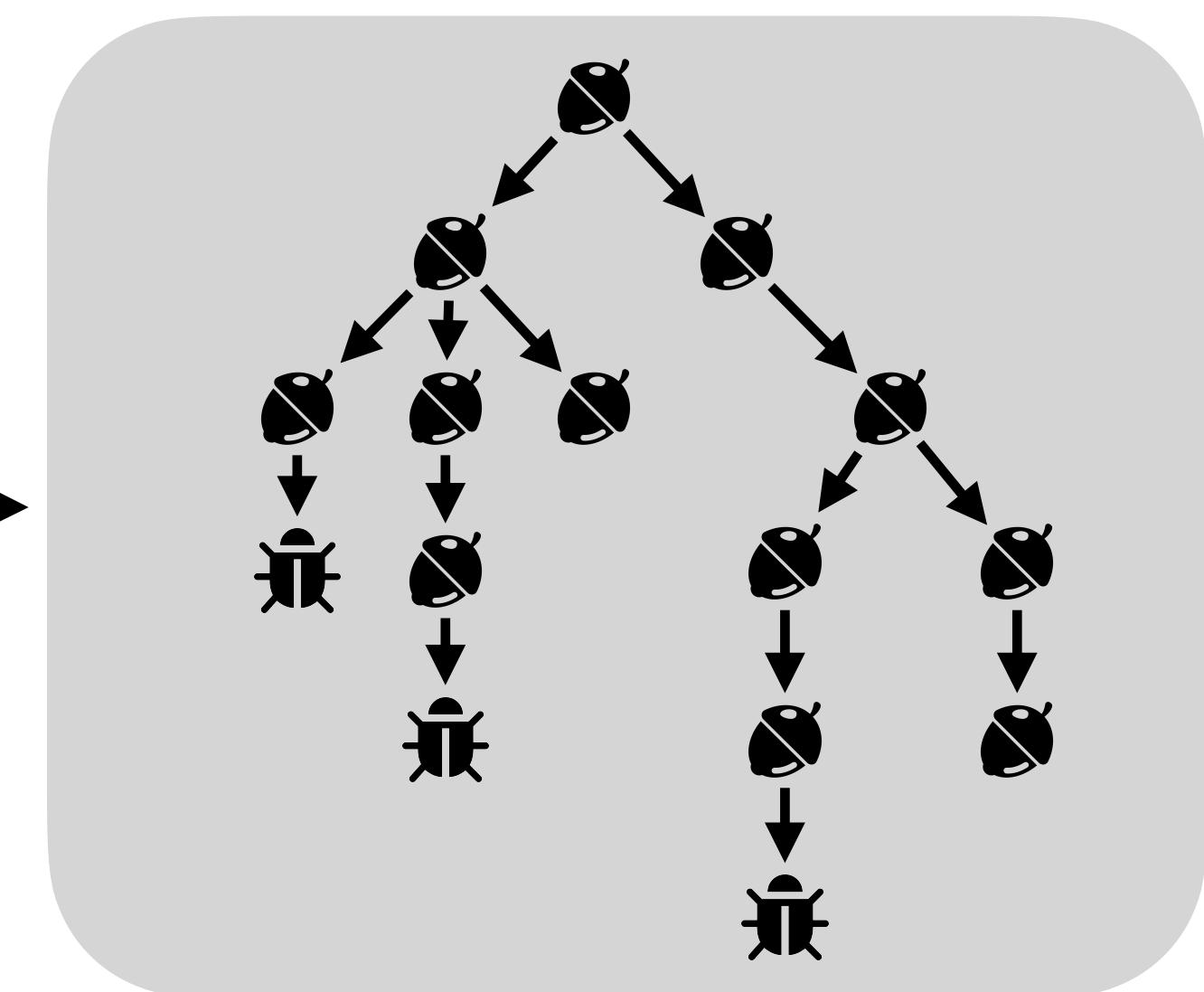
Fuzzing Phase



Data Collection Phase



Visualization Phase



# **Key Challenges**

# **Key Challenges**

## **Data Collection**

# Key Challenges

## Data Collection

- Structure of genealogical tree

# Key Challenges

## Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis

# Key Challenges

## Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

# Key Challenges

## Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

## Visualization

# Key Challenges

## Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

## Visualization

- Graphical visualization of collected data

# Key Challenges

## Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

## Visualization

- Graphical visualization of collected data
- Must be **scalable** and **interactive**

# Data Collection

# **Data Collection**

## **Objectives**

# Data Collection

## Objectives

- Structure of the genealogical tree

# Data Collection

## Objectives

- Structure of the genealogical tree
  - Parent-child relationships between inputs

# Data Collection

## Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata

# Data Collection

## Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata
  - **What** was the progress?

# Data Collection

## Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata
  - **What** was the progress?
  - **How** was the progress made?

# Data Collection

## Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata
  - **What** was the progress?
  - **How** was the progress made?
  - How **difficult** was the progress?

# Data Collection

**Parent-child relationships between inputs**

# Data Collection

## **Parent-child relationships between inputs**

- Naming convention of AFL

# Data Collection

## Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,171,src:000021,op:havoc,rep:2”

# Data Collection

## Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,171,src:000021,op:havoc,rep:2”
  - Input “000027” has input “000021” as a parent

# Data Collection

## Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,171,src:000021,op:havoc,rep:2”
  - Input “000027” has input “000021” as a parent



# Data Collection

## Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,171,src:000021,op:havoc,rep:2”
  - Input “000027” has input “000021” as a parent
- Compatible with 11 out of 14 state-of-the-art Directed Grey-box Fuzzers



# Data Collection

**Metadata per edge**

# Data Collection

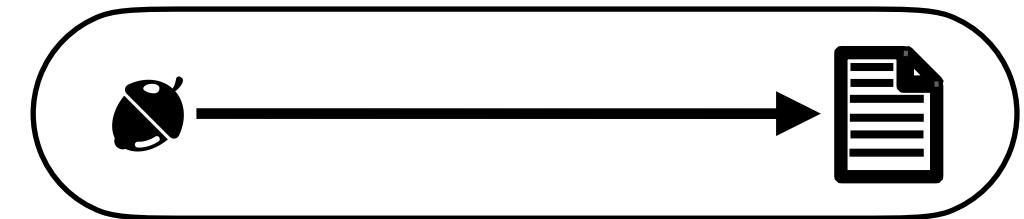
## Metadata per edge

- What was the progress?

# Data Collection

## Metadata per edge

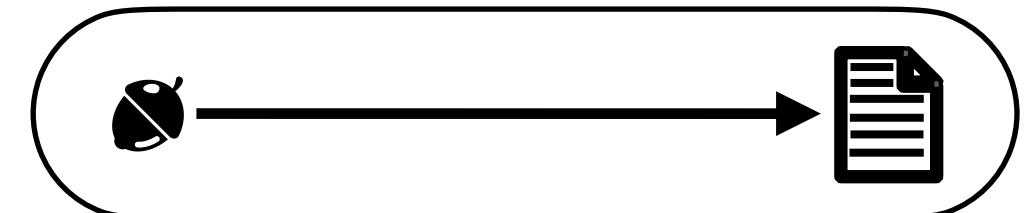
- **What** was the progress?
  - Additional coverage data achieved with new input



# Data Collection

## Metadata per edge

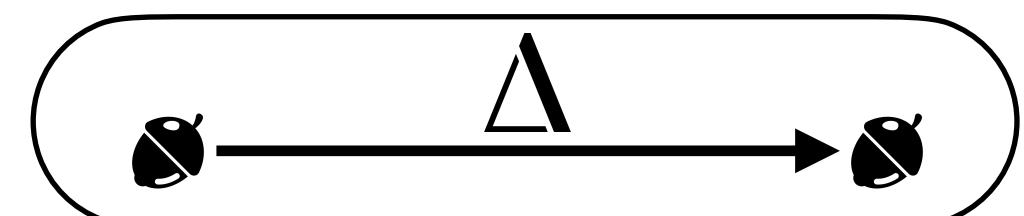
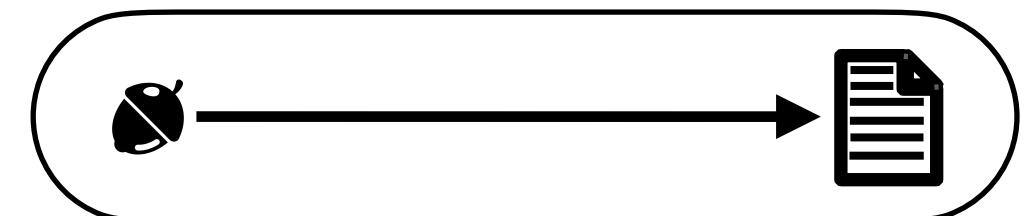
- **What** was the progress?
  - Additional coverage data achieved with new input
- **How** was the progress made?



# Data Collection

## Metadata per edge

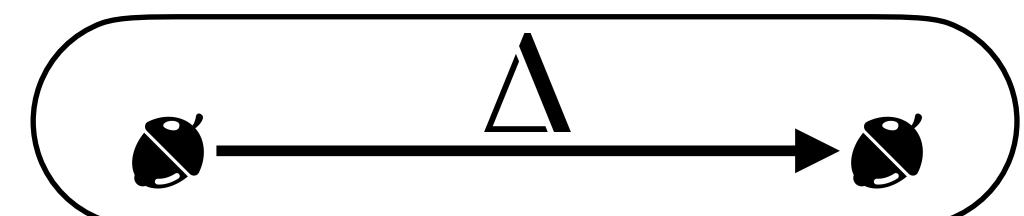
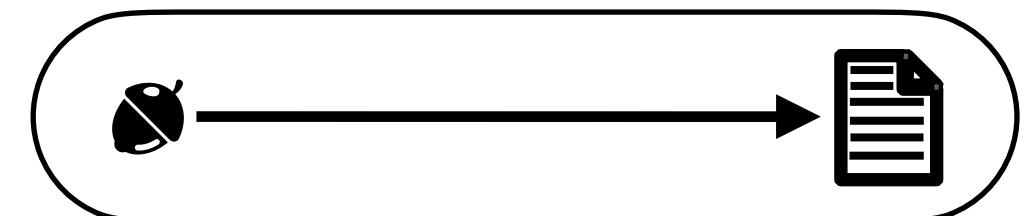
- **What** was the progress?
  - Additional coverage data achieved with new input
- **How** was the progress made?
  - Mutation delta between parent-child inputs



# Data Collection

## Metadata per edge

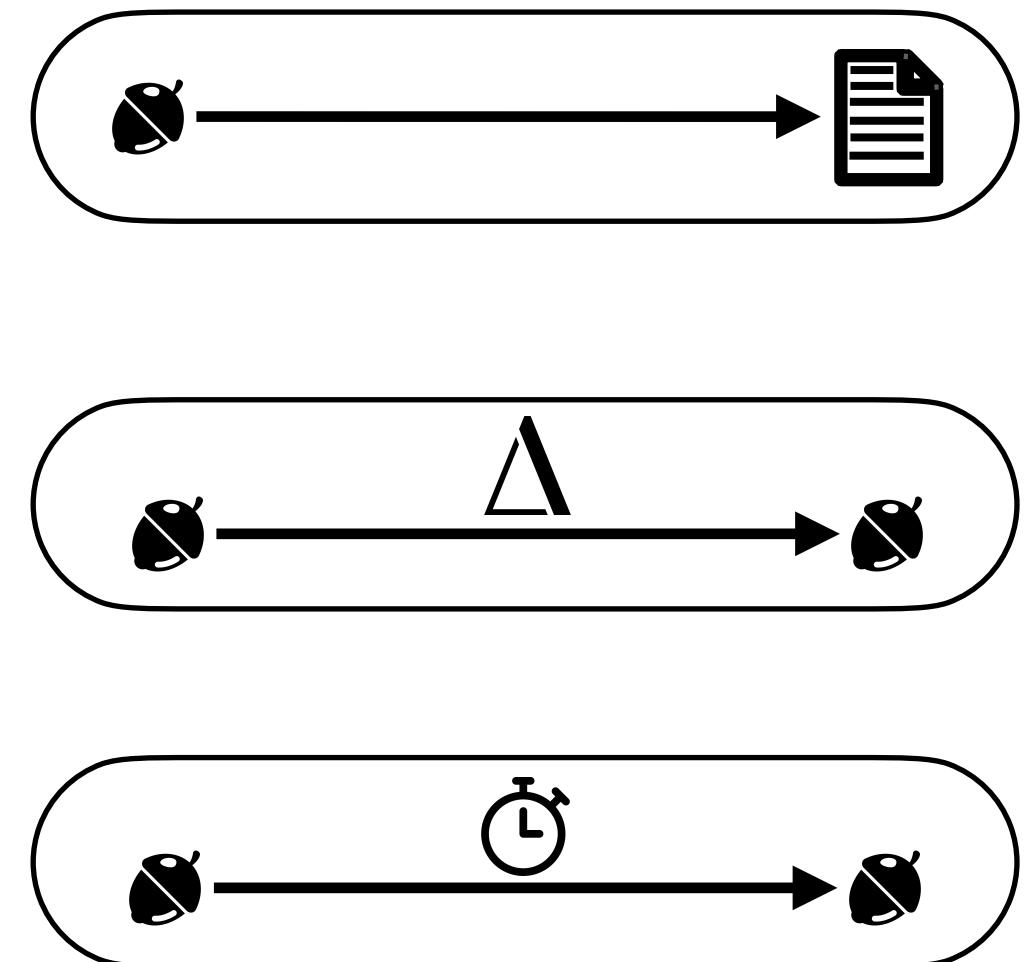
- **What** was the progress?
  - Additional coverage data achieved with new input
- **How** was the progress made?
  - Mutation delta between parent-child inputs
- How **difficult** was the progress?



# Data Collection

## Metadata per edge

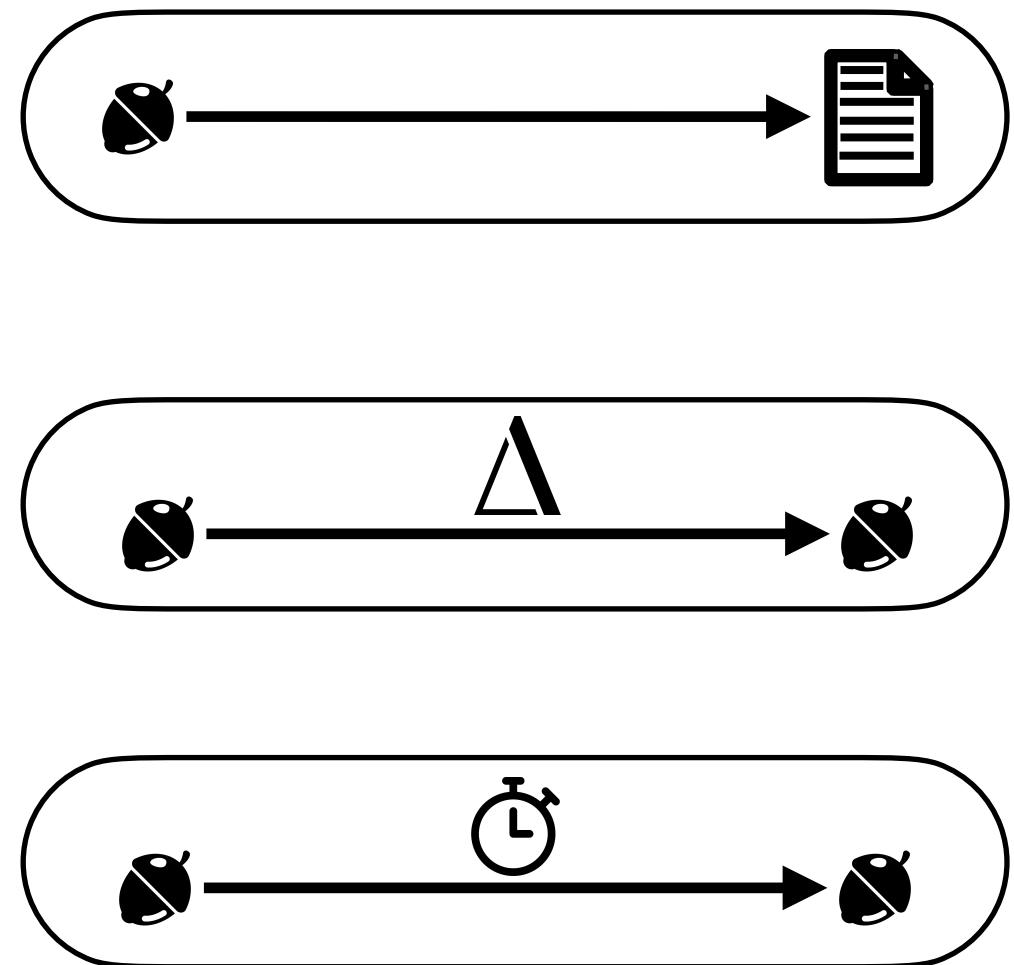
- **What** was the progress?
  - Additional coverage data achieved with new input
- **How** was the progress made?
  - Mutation delta between parent-child inputs
- How **difficult** was the progress?
  - Generation time delta between parent-child inputs



# Data Collection

## Metadata per edge

- **What** was the progress?
  - Additional coverage data achieved with new input
- **How** was the progress made?
  - Mutation delta between parent-child inputs
- How **difficult** was the progress?
  - Generation time delta between parent-child inputs
- Independent from fuzzer implementation



# Visualization

# Visualization

**D3: Data visualization library**

# Visualization

## D3: Data visualization library

- Scalable

# Visualization

## D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format

# Visualization

## D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss

# Visualization

## D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss
- **Interactive**

# Visualization

## D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss
- **Interactive**
  - Supports various interactions

# Visualization

## D3: Data visualization library

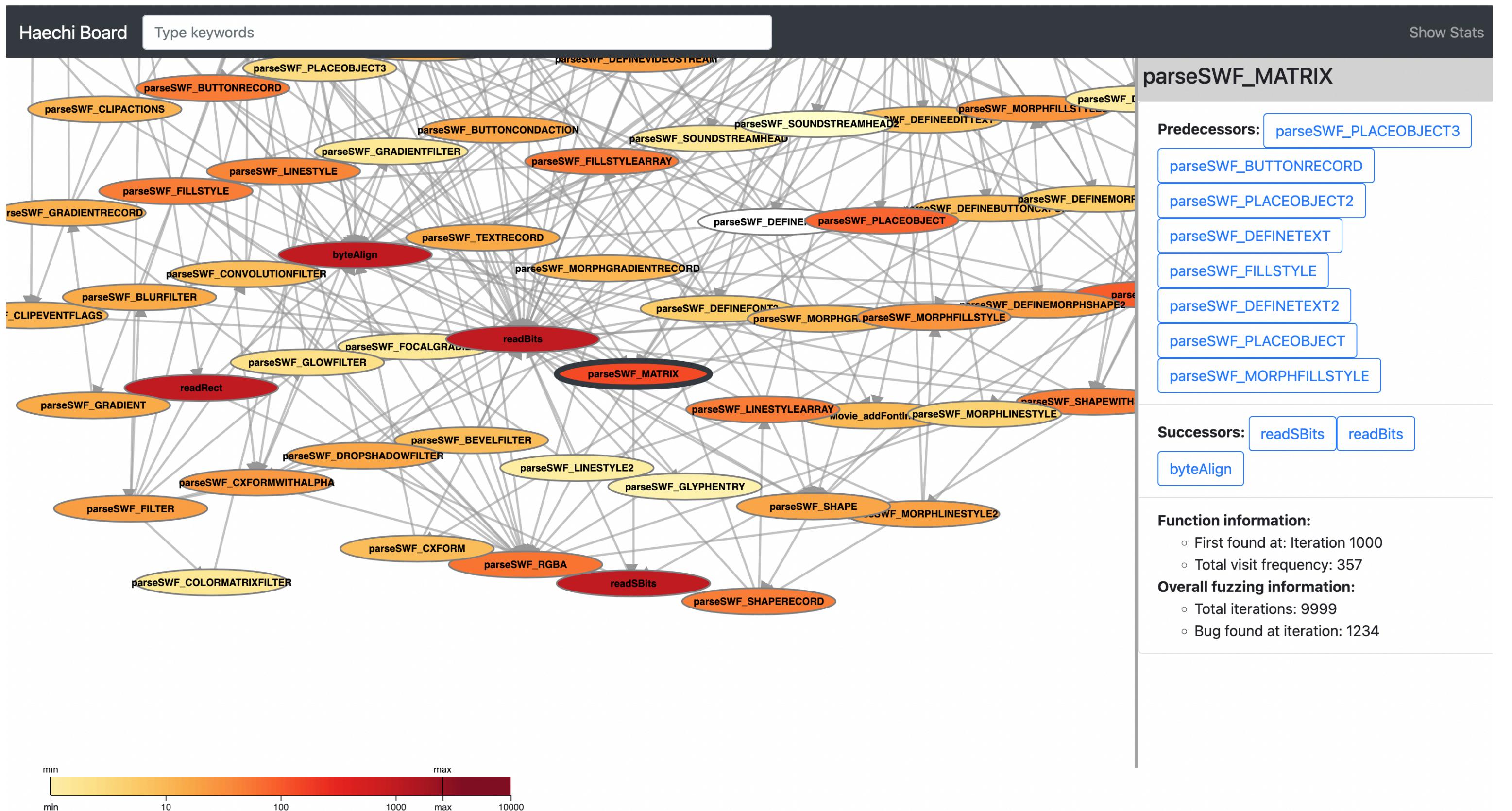
- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss
- **Interactive**
  - Supports various interactions
  - Zoom in/out, toggle, traversing the graph

# Visualization

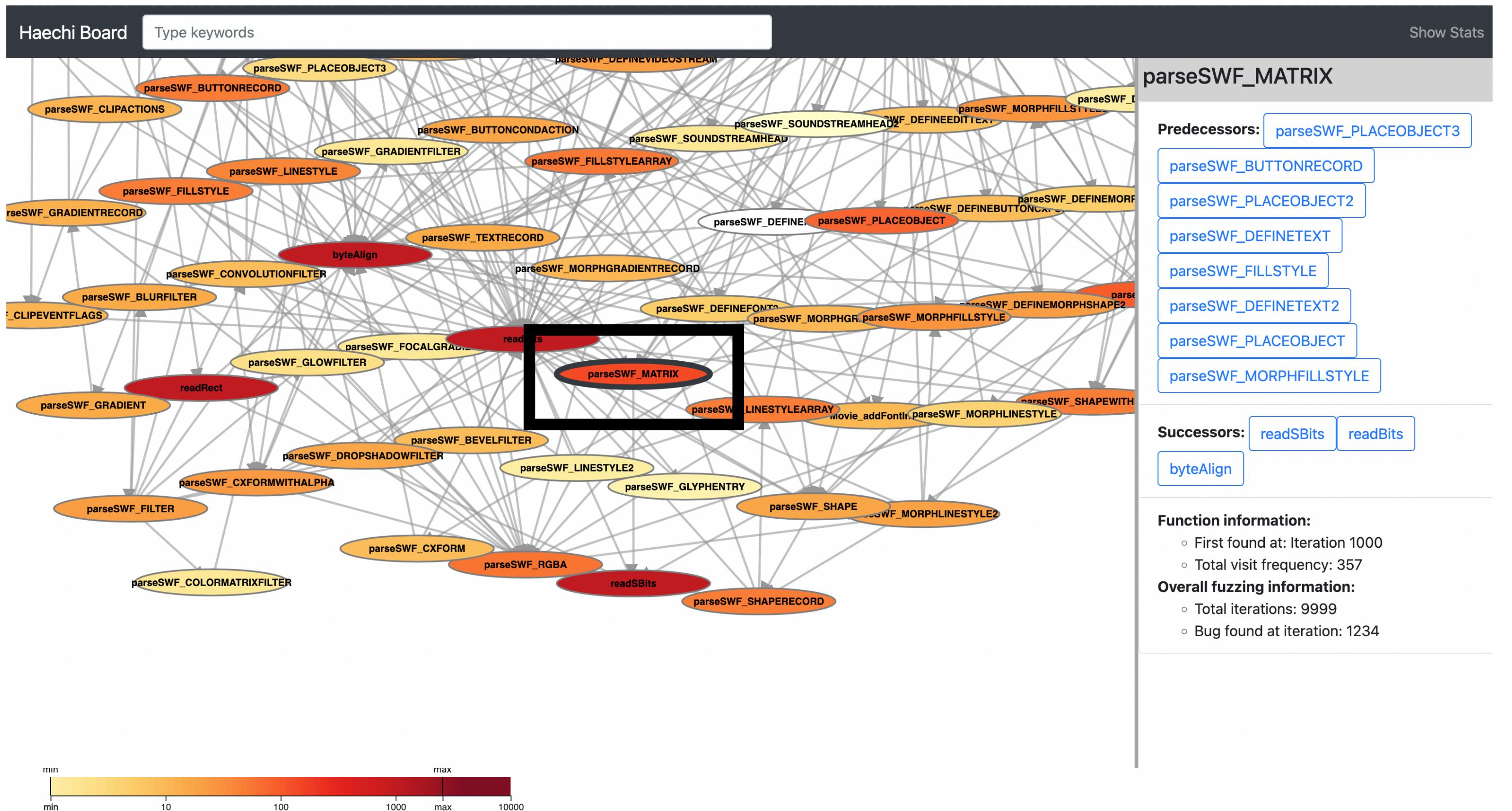
## D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss
- **Interactive**
  - Supports various interactions
  - Zoom in/out, toggle, traversing the graph
- Example: Call graph coverage heat map

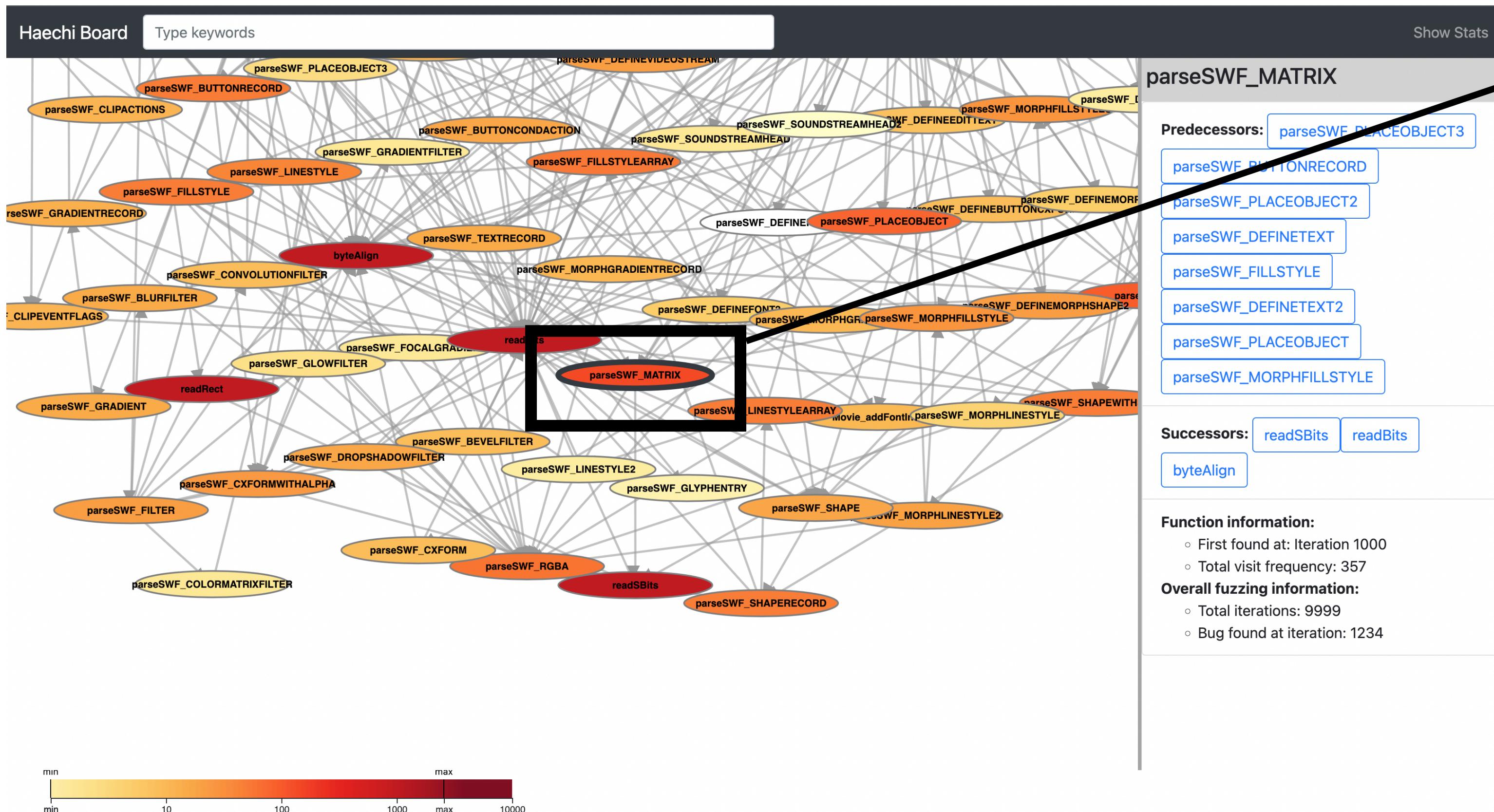
# Visualization



# Visualization

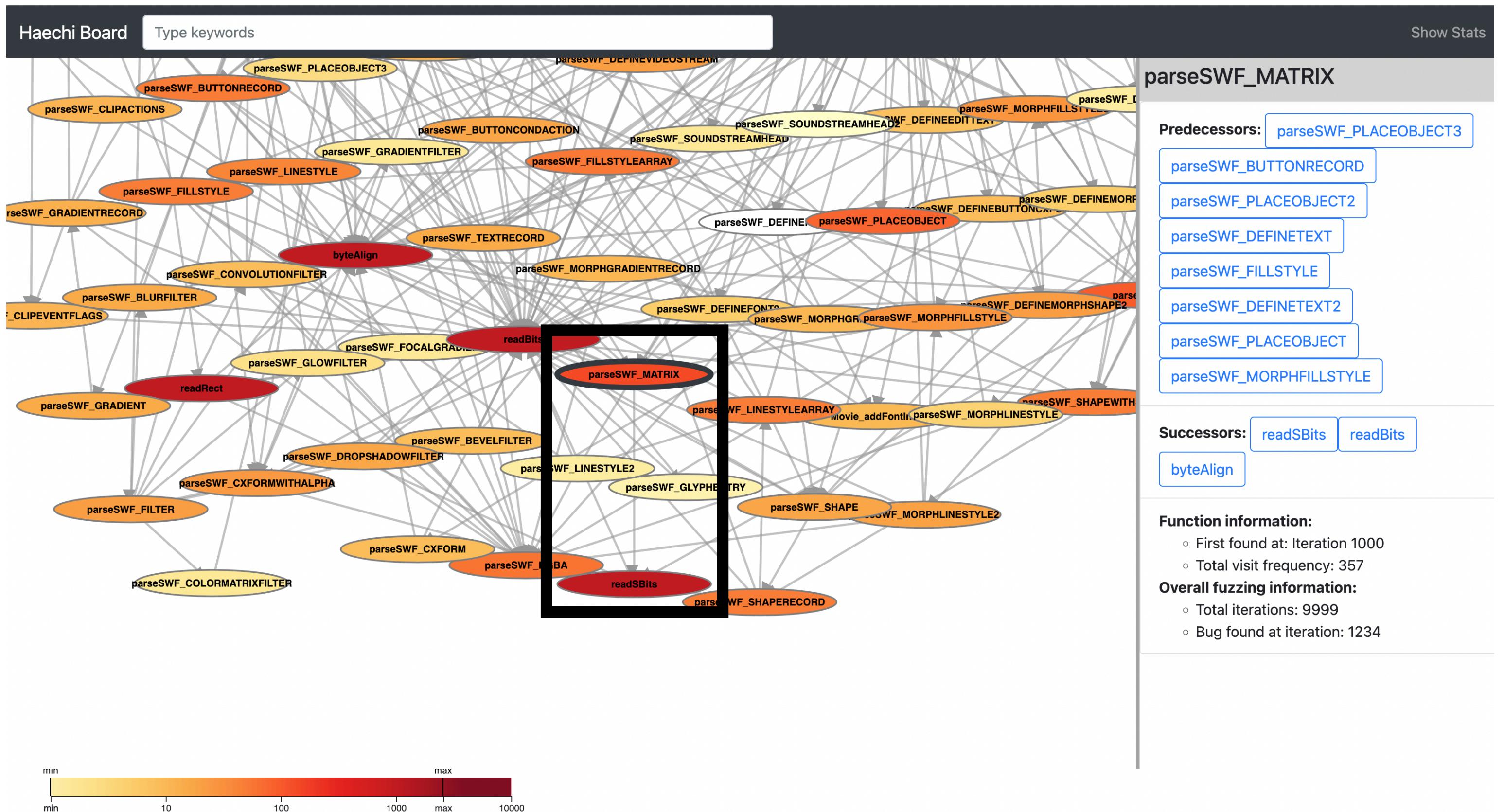


# Visualization



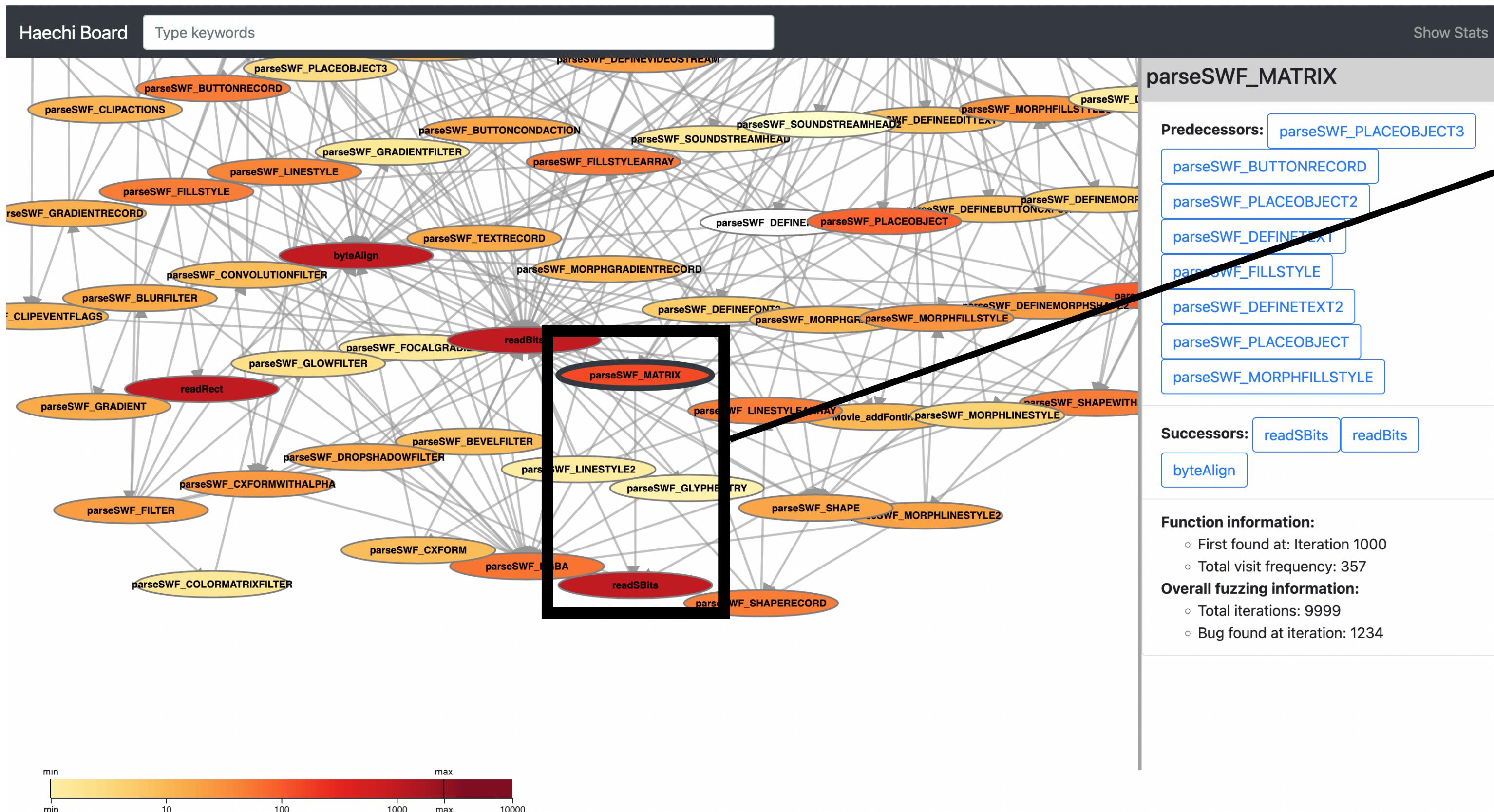
# Node: function

# Visualization



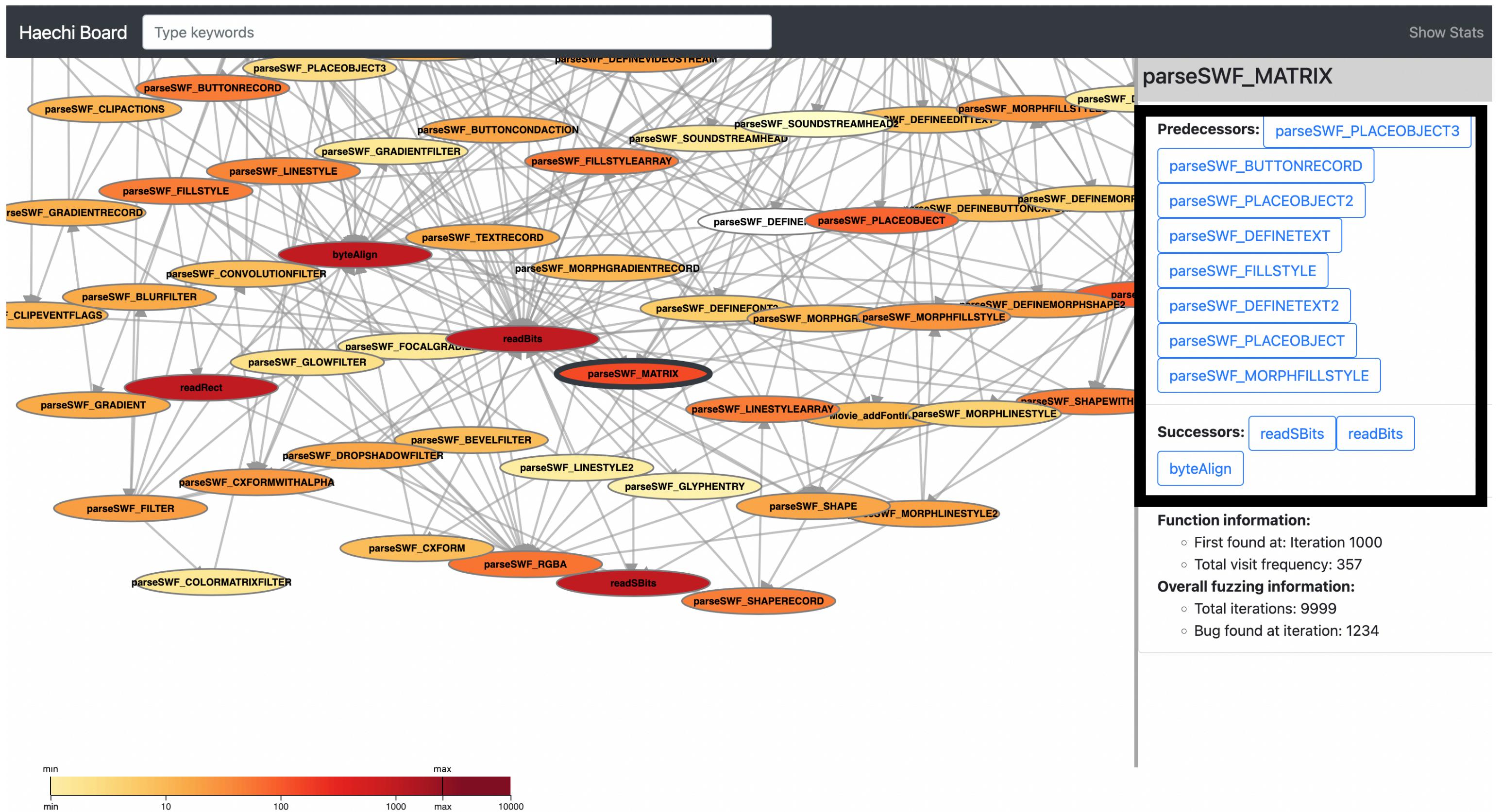
Node: function

# Visualization



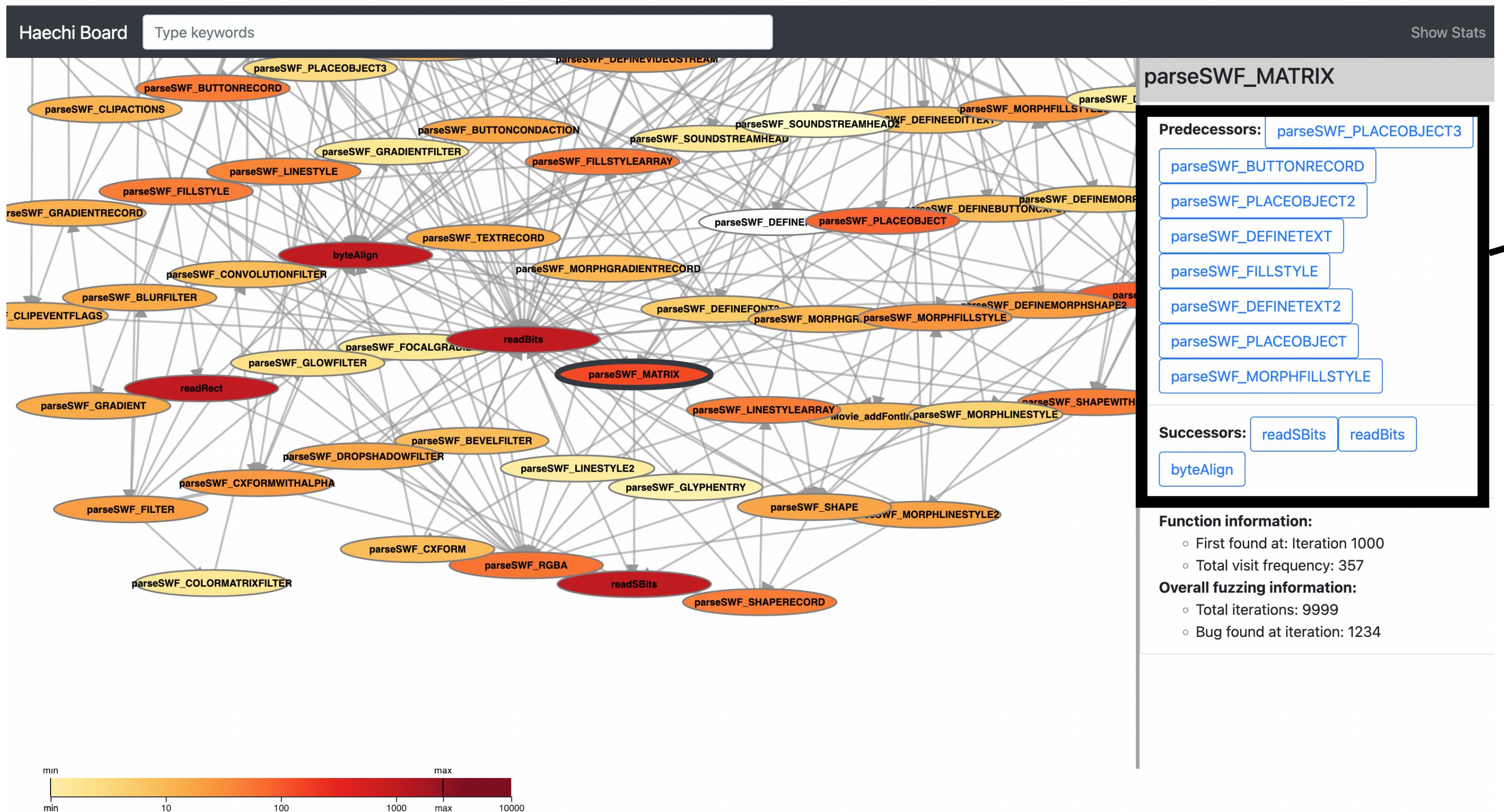
Node: function  
Edge: caller - callee relationship

# Visualization



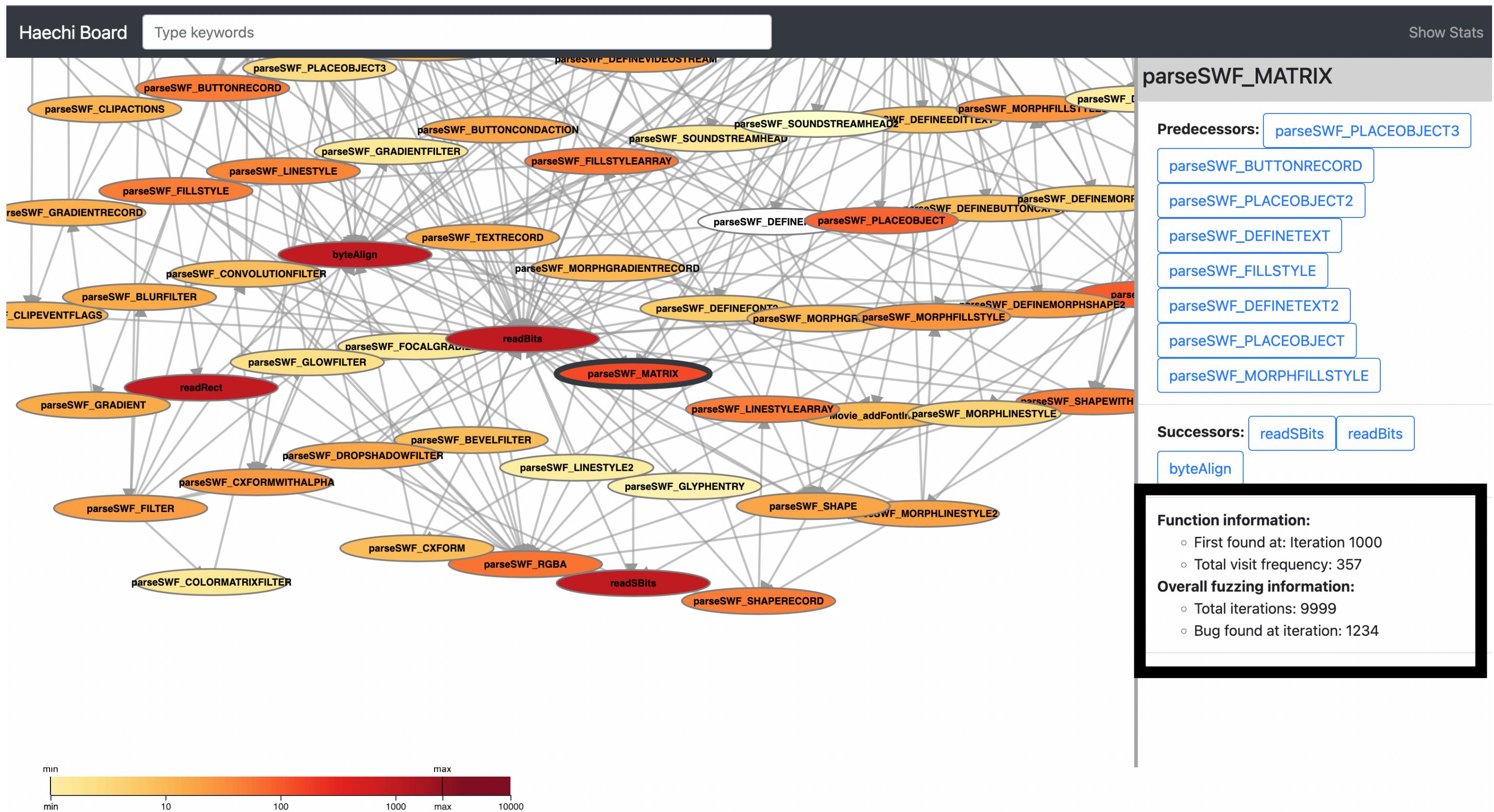
Node: function  
Edge: caller - callee relationship

# Visualization



Node: function  
Edge: caller - callee relationship  
Predecessors, Successors

# Visualization

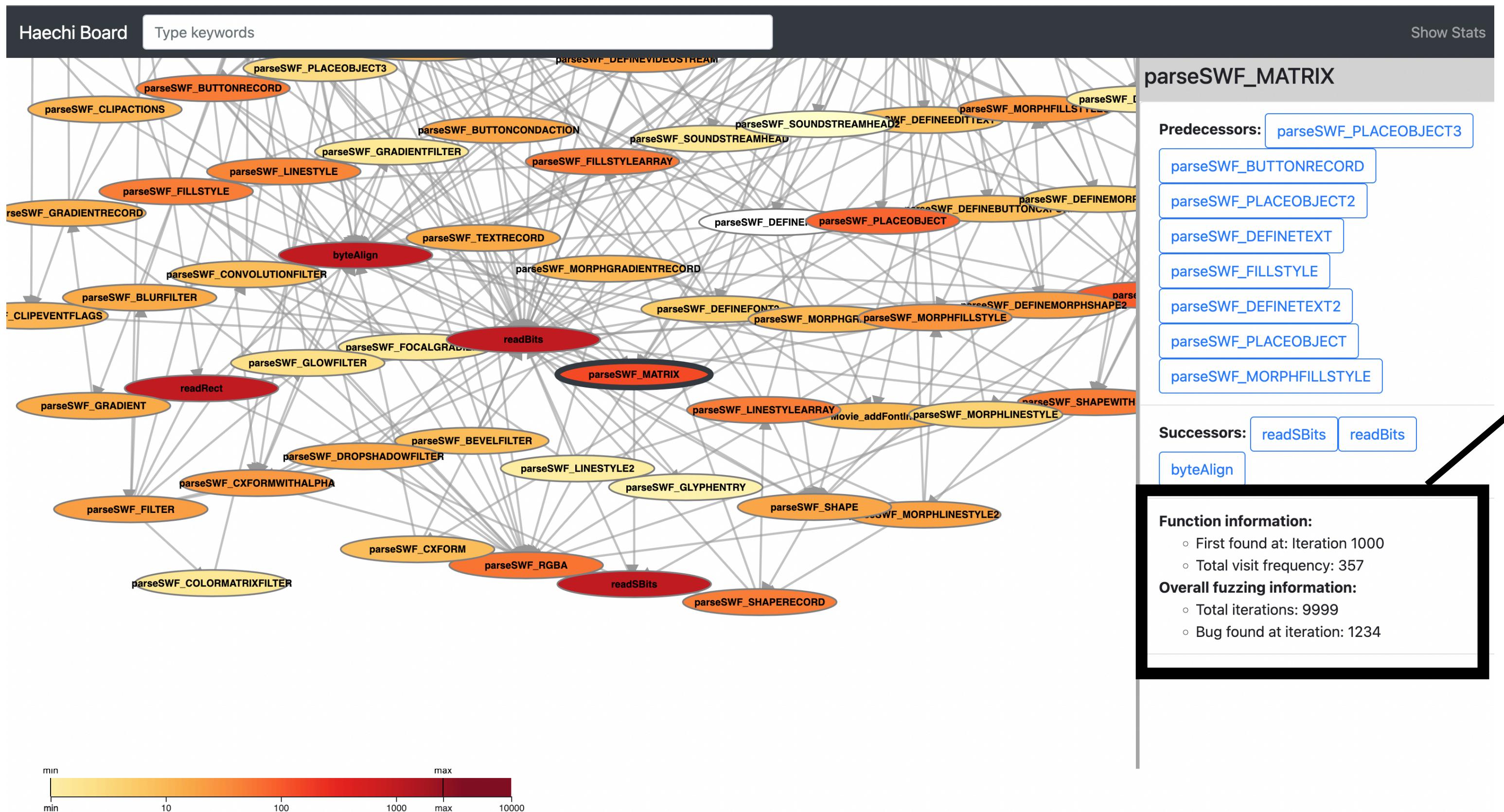


Node: function

Edge: caller - callee relationship

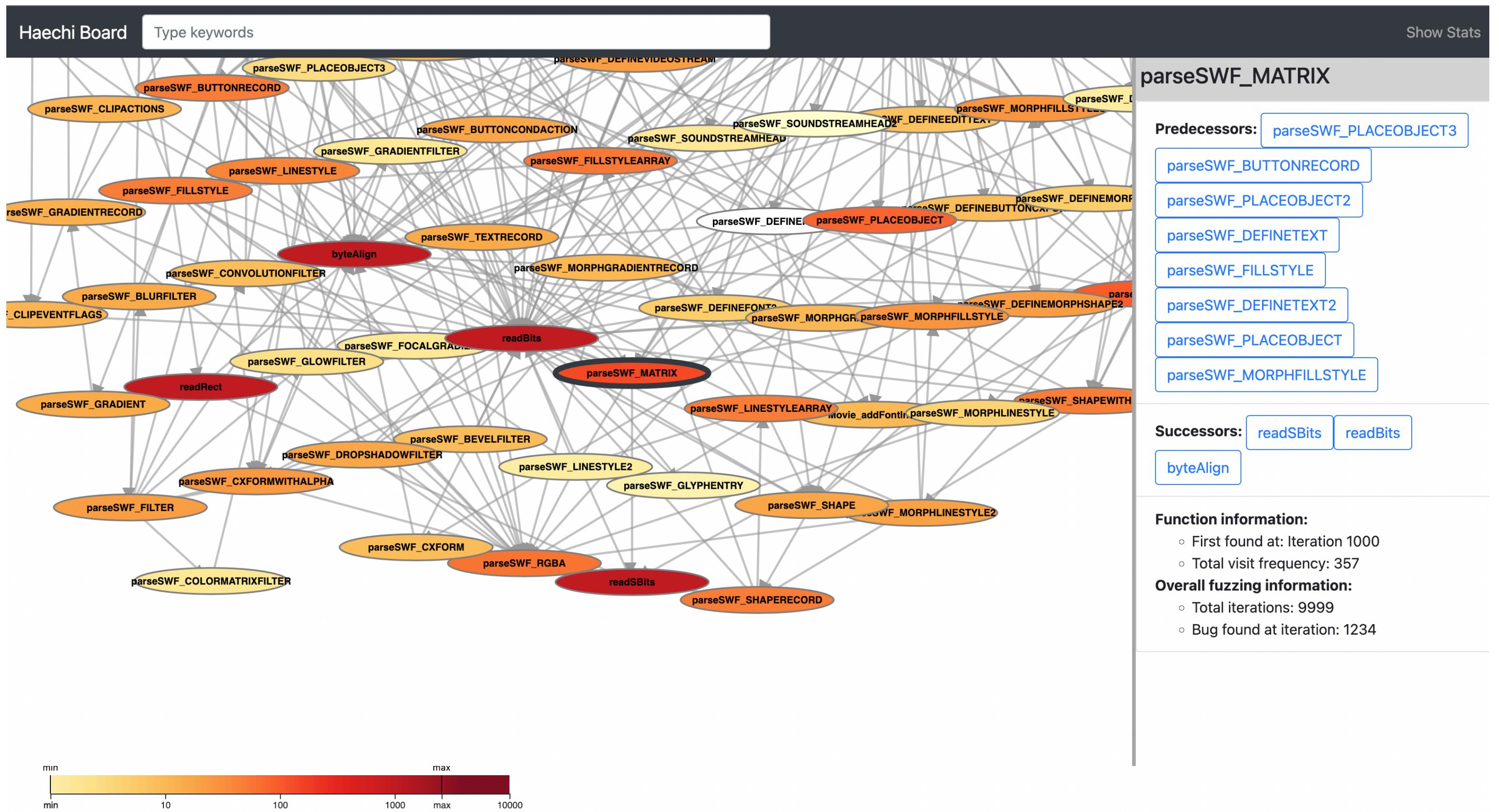
Predecessors, Successors

# Visualization



Node: function  
Edge: caller - callee relationship  
Predecessors, Successors  
Other metadata

# Visualization



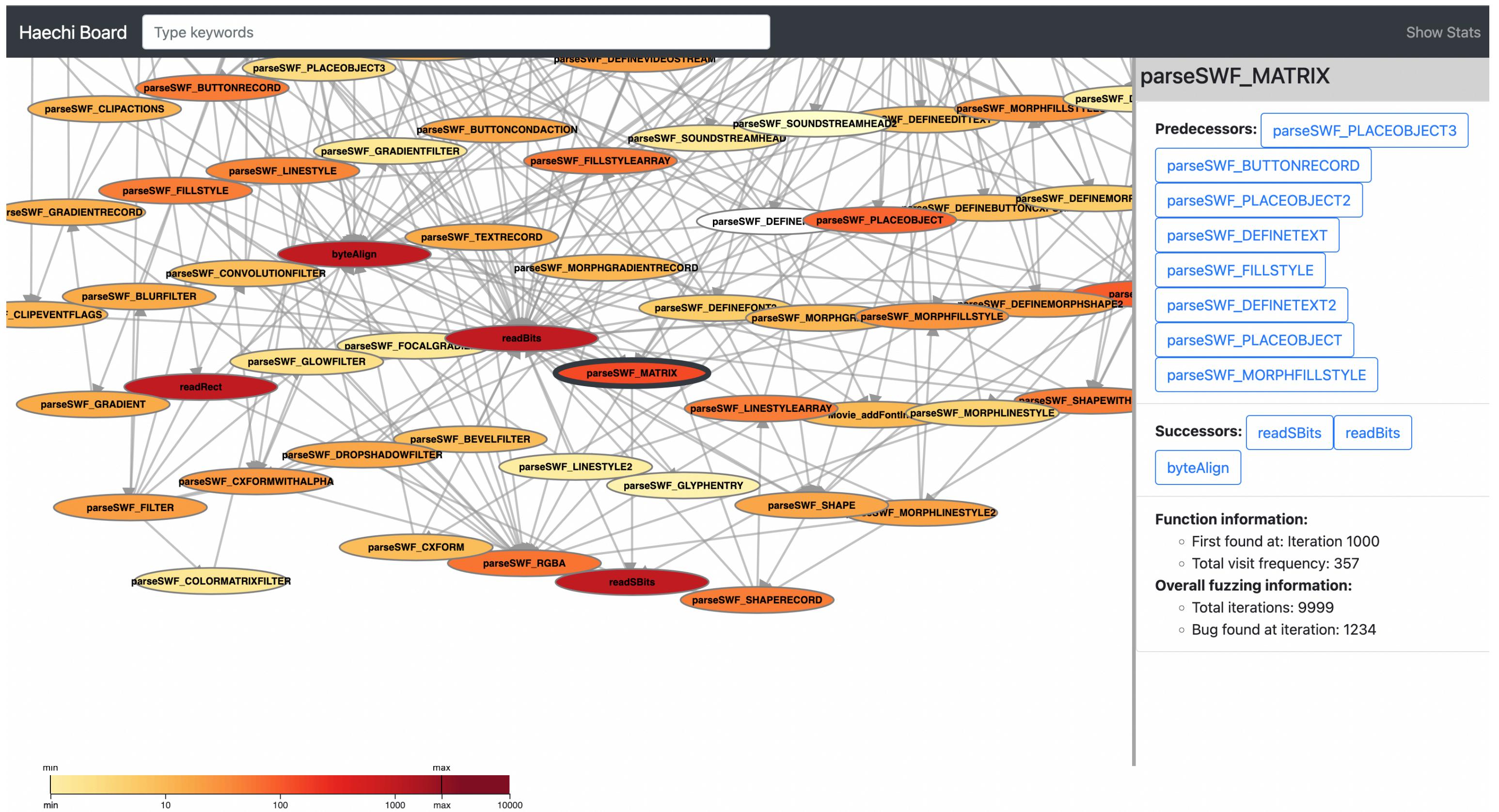
Node: function

Edge: caller - callee relationship

Predecessors, Successors

Other metadata

# Visualization



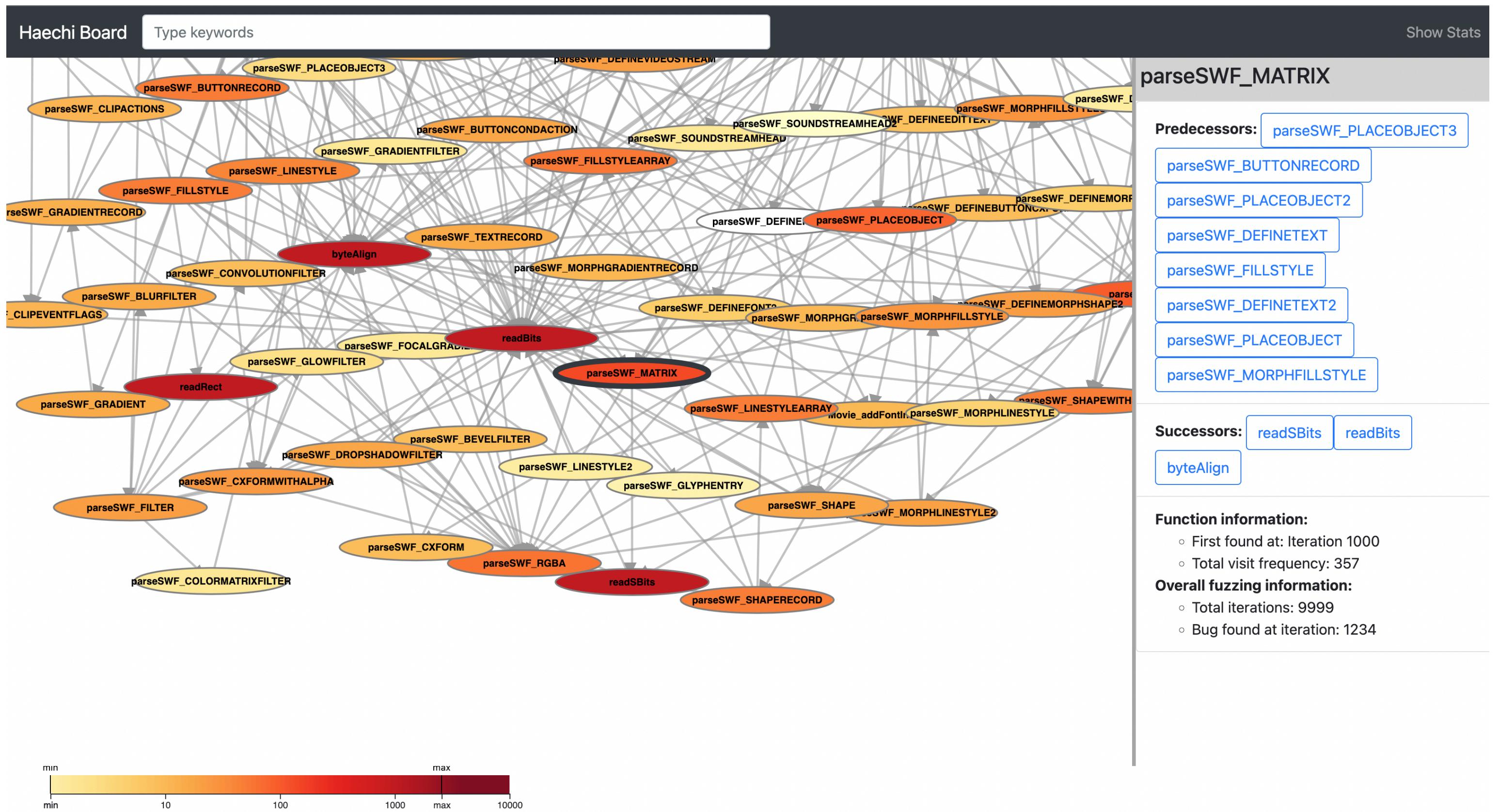
Node: input

Edge: caller - callee relationship

Predecessors, Successors

Other metadata

# Visualization



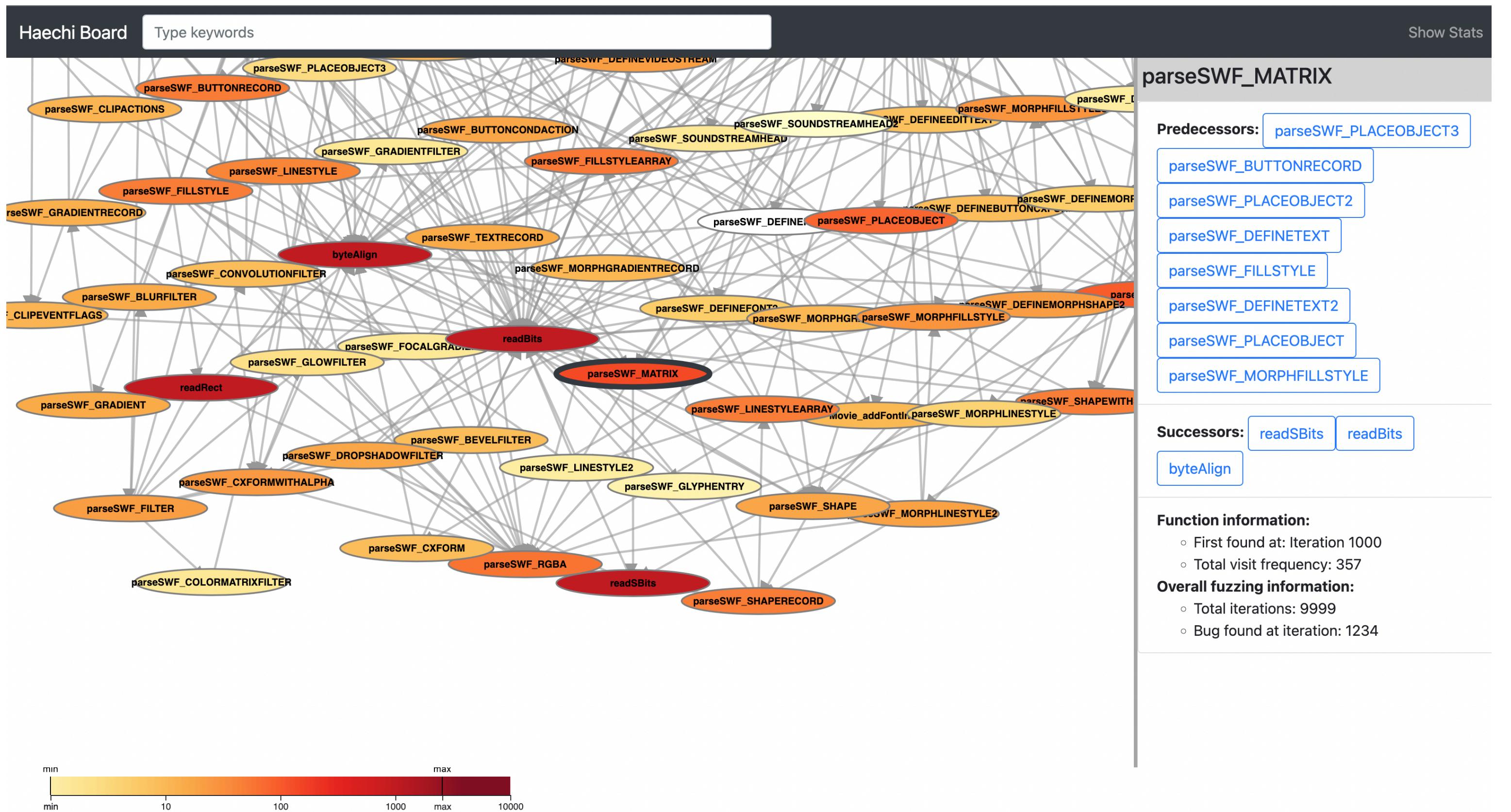
Node: input

Edge: parent - child relationship

Predecessors, Successors

Other metadata

# Visualization



Node: input  
Edge: parent - child relationship  
Parent, Children  
Other metadata

# Expected Results

# Expected Results

**GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

# Expected Results

## **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers

# Expected Results

## **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers
- **Scalable** to large-scale data with no resolution loss

# Expected Results

## **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers
- **Scalable** to large-scale data with no resolution loss
- **Interactive** to provide zoom in/out, toggle, traversing the graph

# Expected Results

## **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers
- **Scalable** to large-scale data with no resolution loss
- **Interactive** to provide zoom in/out, toggle, traversing the graph

## Research Paper

# Expected Results

## **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers
- **Scalable** to large-scale data with no resolution loss
- **Interactive** to provide zoom in/out, toggle, traversing the graph

## **Research Paper**

- Details of the development

# Expected Results

## **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers
- **Scalable** to large-scale data with no resolution loss
- **Interactive** to provide zoom in/out, toggle, traversing the graph

## **Research Paper**

- Details of the development
- Submitted to the top-tier conference or journal

# Our Capabilities

# Our Capabilities

**Extensive experience of Directed Grey-box Fuzzing**

# Our Capabilities

## **Extensive experience of Directed Grey-box Fuzzing**

- Recently introduced DAFL<sup>1</sup>, a state-of-the-art Directed Grey-box Fuzzer

1. “Evaluating Directed Fuzzers: Are We Heading in the Right Direction?”, Kim et al., FSE 2024

# Our Capabilities

## **Extensive experience of Directed Grey-box Fuzzing**

- Recently introduced DAFL<sup>1</sup>, a state-of-the-art Directed Grey-box Fuzzer
  - Downloaded over 470 times in Zenodo

1. “Evaluating Directed Fuzzers: Are We Heading in the Right Direction?”, Kim et al., FSE 2024

# Our Capabilities

## Extensive experience of Directed Grey-box Fuzzing

- Recently introduced DAFL<sup>1</sup>, a state-of-the-art Directed Grey-box Fuzzer
  - Downloaded over 470 times in Zenodo
  - First to investigate the evaluation practice of Directed Grey-box Fuzzing<sup>2</sup>

1. “Evaluating Directed Fuzzers: Are We Heading in the Right Direction?”, Kim et al., FSE 2024
2. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

# Our Capabilities

## Extensive experience of Directed Grey-box Fuzzing

- Recently introduced DAFL<sup>1</sup>, a state-of-the-art Directed Grey-box Fuzzer
  - Downloaded over 470 times in Zenodo
  - First to investigate the evaluation practice of Directed Grey-box Fuzzing<sup>2</sup>

## Experience of Visualization for Fuzzing

1. “Evaluating Directed Fuzzers: Are We Heading in the Right Direction?”, Kim et al., FSE 2024
2. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

# Our Capabilities

## Extensive experience of Directed Grey-box Fuzzing

- Recently introduced DAFL<sup>1</sup>, a state-of-the-art Directed Grey-box Fuzzer
  - Downloaded over 470 times in Zenodo
  - First to investigate the evaluation practice of Directed Grey-box Fuzzing<sup>2</sup>

## Experience of Visualization for Fuzzing

- Developed heat map of call graph coverage

1. “Evaluating Directed Fuzzers: Are We Heading in the Right Direction?”, Kim et al., FSE 2024
2. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

# **Summary**

# Summary

- Challenges in analyzing Directed Grey-box Fuzzing

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users
- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users
- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users
- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users
- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users
- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive
- **Contributions**

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users
- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive
- **Contributions**
  - Enable precise analysis of the performance of Directed Grey-box Fuzzing

# Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users
- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive
- **Contributions**
  - Enable precise analysis of the performance of Directed Grey-box Fuzzing
  - Open up the opportunity to further improve the field of Directed Grey-box Fuzzing