

No Symbols? No Problem!

By Max ‘Libra’ Kersten

Table of contents

- About me
- Symbols and types of code
- Symbol recovery
- Bulk signature generation
- Case study
- Methodology

About me

- Max ‘Libra’ Kersten (/in/Libranalysis on LinkedIn, @Libranalysis on Twitter)
  - Spoke at numerous conferences (BlackHat USA/EU/MEA/Asia, DEFCON, Botconf, and others)
- Malware analyst at Trellix’ Advanced Research Center
  - Published DotDumper
- I write blogs about reverse engineering
  - Including my free Binary Analysis Course
- My tools are open-sourced on GitHub
  - Such as AndroidProjectCreator and the Mobile Malware Mimicking Framework

Trellix

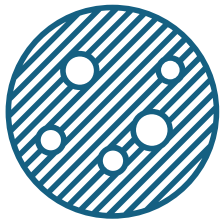
Symbols 101



Recognisable



Self-explanatory



Unambiguous

Symbols 101



Recognisable



Self-explanatory



Unambiguous

Types of code



Runtime



Library



User

Symbol recovery



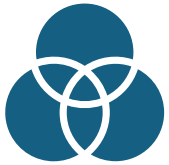
Metadata

Useful, but not always available



FunctionID

Function name and hash mapping



BSim

Used to see overlap between functions

FunctionID databases

- Automated
- Runs headless

```
INFO  HEADLESS: execution starts (HeadlessAnalyzer)
INFO  Opening existing project: C:\Users\malwa\fidb-test (HeadlessAnalyzer)
INFO  Opening project: C:\Users\malwa\fidb-test (HeadlessProject)
INFO  SCRIPT: C:\Users\malwa\ghidra_scripts\AutomaticallyCreateFunctionIdDatabases.java (HeadlessAnalyzer)
INFO  AutomaticallyCreateFunctionIdDatabases.java> Received project name: projectName (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> Received project version: projectVersion (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> Received output folder path: C:\Users\malwa\Desktop\fidb (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> Received choice with regards to the usage of a common symbols file: false (Ghidra
INFO  AutomaticallyCreateFunctionIdDatabases.java> Collected language IDs and their versions:
        x86:LE:32:default (4.0)
 (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> x86:LE:32:default contains 3 files
 (GhidraScript)
INFO  Packed database cache: C:\Users\malwa\AppData\Local\ghidra\packed-db-cache (PackedDatabaseCache)
INFO  AutomaticallyCreateFunctionIdDatabases.java> [x86:LE:32:default] Generating "projectName (projectVersion)" based on 3 files (G
INFO  AutomaticallyCreateFunctionIdDatabases.java> projectName:projectVersion:x86:LE:32:default (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> 164 total functions visited (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> 42 total functions added (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> 122 total functions excluded (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> Breakdown of exclusions: (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java>     FAILED_FUNCTION_FILTER: 0 (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java>     MEMORY_ACCESS_EXCEPTION: 0 (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java>     IS_THUNK: 0 (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java>     FAILS_MINIMUM_SHORTHASH_LENGTH: 0 (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java>     NO_DEFINED_SYMBOL: 122 (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java>     DUPLICATE_INFO: 0 (GhidraScript)
INFO  AutomaticallyCreateFunctionIdDatabases.java> List of unresolved symbols: (GhidraScript)
```

Case study

- Default analysis
- Post FunctionID

```
101  FUN_004e8b20();
102  FUN_004e8b20();
103  FUN_004e88e0();
104  FUN_004e8b20();
105  FUN_004e8880();
106  *param_10 = extraout_R10_01;
107  param_10[1] = extraout_R11_01;
108  param_10[2] = uVar8;
109  param_10[3] = uVar5;
110  FUN_004e8880();
111  FUN_004e88e0();
112  FUN_004e8880();
```

```
101  FUN_004e8b20();
102  FUN_004e8b20();
103  FUN_004e88e0();
104  FUN_004e8b20();
105  p256SubInternal();
106  *param_10 = extraout_R10_01;
107  param_10[1] = extraout_R11_01;
108  param_10[2] = uVar8;
109  param_10[3] = uVar5;
110  p256SubInternal();
111  FUN_004e88e0();
112  p256SubInternal();
```

BSim databases

- Shoehorned
- Automated
- Runs headless

```
<description layout_version="5" major="6" minor="0" settings="0x4d">
<execlist>
<exe>
  <md5>0000a1bccd58d63b924f45dd8ef21ff5</md5>
  <name>curve448-mul-g.obj</name>
  <arch>x86:LE:32:default</arch>
  <compiler>windows</compiler>
  <date millis="0x6">0x65a5a6ba</date>
  <repository>ghidra:/F:/ghidraProjects/libnettle/libnettle</repository>
  <path>libnettle/libnettle_nettle_3.8_release_20220602_msvc15/bin/x86</path>
</exe>
<fdesc name="_nettle_curve448_mul_g" addr="0x2d00">
<lshcosine>
 <hash tf="15">0xbe28207</hash>
 <hash>0x142f8cda</hash>
 <hash>0x2d00064e</hash>
 <hash tf="6">0x3d209d83</hash>
 <hash>0x3fa0950c</hash>
 <hash>0x417e5477</hash>
 <hash tf="6">0x4d88e700</hash>
 <hash>0x4ef74828</hash>
 <hash>0x51f32399</hash>
 <hash tf="26">0x545c6155</hash>
 <hash>0x55123056</hash>
 <hash>0x6c176aad</hash>
 <hash>0x7257ef6c</hash>
 <hash>0x90790e2c</hash>
 <hash tf="9">0x967ef100</hash>
 <hash>0xa150976f</hash>
 <hash tf="7">0xa45c1d72</hash>
 <hash>0xab3b5a1e</hash>
 <hash>0xabef06bb</hash>
 <hash>0xc87aca45</hash>
 <hash>0xf0522b88</hash>
</lshcosine>
<call dest="@__security_check_cookie@4">
  <name>unknown</name>
  <compiler></compiler>
</call>
<call dest="__nettle_curve448_eh_to_x">
  <name>unknown</name>
  <compiler></compiler>
</call>
<call dest="__nettle_ecc_mul_g_eh">
  <name>unknown</name>
  <compiler></compiler>
</call>
<call dest="__nettle_gmp_alloc_limbs">
  <name>unknown</name>
  <compiler></compiler>
</call>
```

BSim matches

- Provide context
- Identical matches
  - Renamed as-is

Decompile: crypto/elliptic.p256PointDoubleAsm - (qbit_258f9a7bab553b4731da8913be33134ec29fe3...

```
1
2  /* Old name: FUN_004e9ba0
3
4     Detected name: "crypto/elliptic.p256PointDoubleAsm"
5
6     Original file, similarity, significance, architecture
7      emptyProject_go1.9rc1_windows_amd64  1  251.462  x86:LE:64:default
8      emptyProject_go1.9.2rc2_windows_amd64  1  251.462  x86:LE:64:default
9      emptyProject_go1.9.2_windows_amd64  1  251.462  x86:LE:64:default
10     emptyProject_go1.16beta1_windows_amd64  1  251.462  x86:LE:64:default
11     emptyProject_go1.15beta1_windows_amd64  1  251.462  x86:LE:64:default
12     emptyProject_go1.15.5_windows_amd64  1  251.462  x86:LE:64:default
13     emptyProject_go1.15.15_windows_amd64  1  251.462  x86:LE:64:default
14     emptyProject_go1.15.14_windows_amd64  1  251.462  x86:LE:64:default
15     emptyProject_go1.14beta1_windows_amd64  1  251.462  x86:LE:64:default
16     emptyProject_go1.14.3_windows_amd64  1  251.462  x86:LE:64:default
17     emptyProject_go1.14.14_windows_amd64  1  251.462  x86:LE:64:default
18     emptyProject_go1.13rc1_windows_amd64  1  251.462  x86:LE:64:default
19     emptyProject_go1.13.7_windows_amd64  1  251.462  x86:LE:64:default
20     emptyProject_go1.13.15_windows_amd64  1  251.462  x86:LE:64:default
21     emptyProject_go1.12rc1_windows_amd64  1  251.462  x86:LE:64:default
22     emptyProject_go1.12.9_windows_amd64  1  251.462  x86:LE:64:default
23     emptyProject_go1.12.8_windows_amd64  1  251.462  x86:LE:64:default
24     emptyProject_go1.12.7_windows_amd64  1  251.462  x86:LE:64:default
25     emptyProject_go1.12.2_windows_amd64  1  251.462  x86:LE:64:default
26     emptyProject_go1.12.13_windows_amd64  1  251.462  x86:LE:64:default */
27
28 void crypto/elliptic.p256PointDoubleAsm
```

BSim matches

- Provide context
- Generic matches
  - Renamed with a prefix

Decompile: golang_FUN_004d0b60 - (qbit_258f9a7bab553b4731da8913be33134ec29fe3061f...

```
/* Old name: golang_FUN_004d0b60

   Old name: FUN_004d0b60

   Detected name: "crypto/internal/nistec/fiat::crypto/internal/nistec/fiat.p384Add"

   Original file, similarity, significance, architecture
    emptyProject_go1.19_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.8_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.6_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.5_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.4_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.3_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.2_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.1_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.13_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.12_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.11_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.19.10_windows_amd64  0.856  134.93  x86:LE:64:default

   Detected name: "crypto/elliptic/internal/fiat::crypto/elliptic/internal/fiat.p384Add"

   Original file, similarity, significance, architecture
    emptyProject_go1.18_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.18.9_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.18.8_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.18.6_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.18.5_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.18.3_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.18.2_windows_amd64  0.856  134.93  x86:LE:64:default
    emptyProject_go1.18.10_windows_amd64  0.856  134.93  x86:LE:64:default */

void golang_FUN_004d0b60(uint *param_1,uint *param_2,uint *param_3,undefined param_4,
```

Case study

- Post FunctionID
- Post BSim

```
101  FUN_004e8b20();
102  FUN_004e8b20();
103  FUN_004e88e0();
104  FUN_004e8b20();
105  p256SubInternal();
106  *param_10 = extraout_R10_01;
107  param_10[1] = extraout_R11_01;
108  param_10[2] = uVar8;
109  param_10[3] = uVar5;
110  p256SubInternal();
111  FUN_004e88e0();
112  p256SubInternal();
```

```
128  golang_FUN_004e8b20();
129  golang_FUN_004e8b20();
130  golang_FUN_004e88e0();
131  golang_FUN_004e8b20();
132  p256SubInternal();
133  *param_10 = extraout_R10_01;
134  param_10[1] = extraout_R11_01;
135  param_10[2] = uVar8;
136  param_10[3] = uVar5;
137  p256SubInternal();
138  golang_FUN_004e88e0();
139  p256SubInternal();
```

Bulk

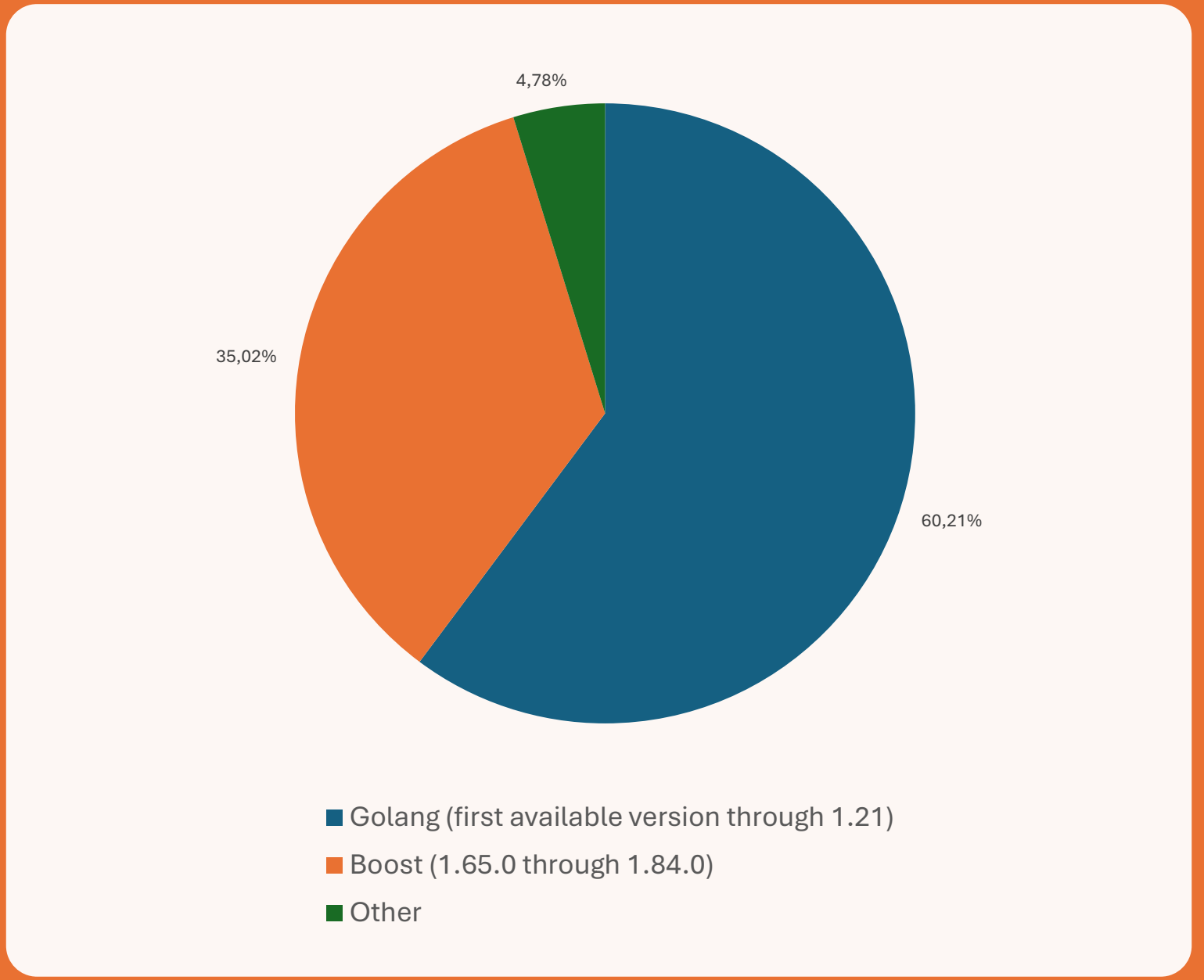


Hundreds of gigabytes of benign binaries



117 GiB of BSim signatures

Bulk FunctionID signature generation



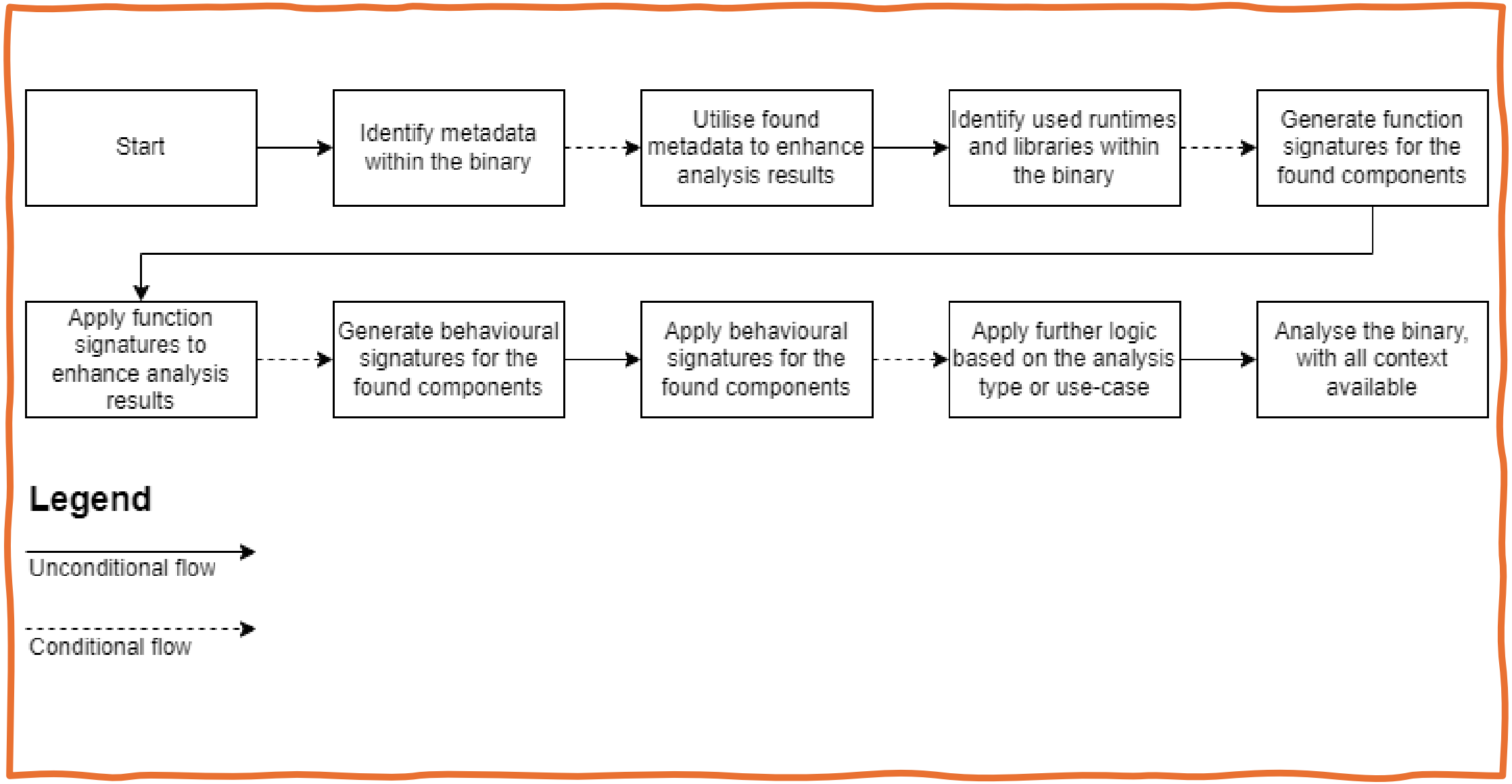
Bulk signature generation

Project name	FunctionID signatures
Golang (first available version through 1.21)	48,472,262
Boost (1.65.0 through 1.84.0)	28,191,439
libxml2	1,608,164
openssl	818,210
libgcrypt	673,280
libnettle	447,443
liblzma	108,279
msvc-empty	86,479
uclibc	47,394
libzlib	16,292
libsodium	16,093
avr-libc	15,616
libbzip2	7,433

Case study: qBit stealer

Step	Recovered symbols
Default analysis	1/2016 (0.05%)
FunctionID recovery	850/2015 (42.2%)
Bsim recovery	319/2015 (15.8%)
Total	1169/2015 (58.0%)

```
import (
	"flag"
	"fmt"
	"github.com/gizak/termui/v3"
	"github.com/gizak/termui/v3/widgets"
	"log"
	"os"
	"sync"
	"time"
)
```


Start
Identify metadata within the binary
Utilise found metadata to enhance analysis results
Identify used runtimes and libraries within the binary
Generate function signatures for the found components
Apply function signatures to enhance analysis results
Generate behavioural signatures for the found components
Apply behavioural signatures for the found components
Apply further logic based on the analysis type or use-case
Analyse the binary, with all context available
Legend
Unconditional flow
Conditional flow

Questions?

- info@maxkersten.nl
- /in/Libranalysis on LinkedIn
- @Libranalysis on Twitter

- https://github.com/advanced-threat-research/
  - GhidraScripts
  - FIDBs
  - BSim
  - Golang-Runtime-Binaries