CUJO AI

VB2021 localhost
October 2021

Reversing Golang Binaries with Ghidra

Dorka Palotay
Senior Threat Researcher, CUJO AI

Albert Zsigovits
Threat Researcher, CUJO AI

Who are we

Background

Albert Zsigovits (@albertzsigovits):

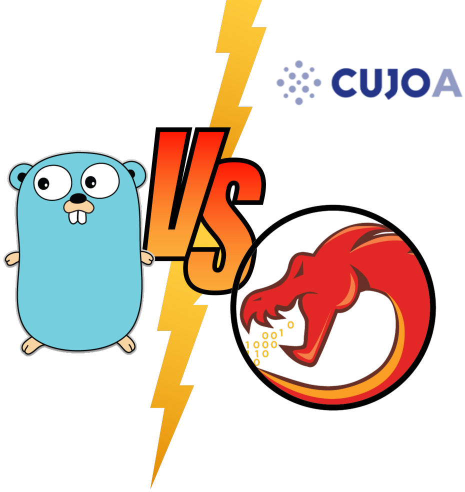
- Threat Researcher @ CUJO AI
- Traditional blue team background
- Top 32 Influential Malware Research Professional 2019
- Memory forensicator, malware analyst and reverse engineer
- Former speaker at SEC-T and Disobey.Fi

Dorka Palotay (@pad0rka):

- Senior Threat Researcher at CUJO AI
- BSc in Applied Mathematics
- MSc in Security and Privacy – Advanced Cryptography
- Worked at financial and security companies as well
- Malware researcher and reverse engineer

Why we did all this

The quest



Background:

- IoT malware research -> more and more (IoT) malware families are written in Go

Issue:

- Reverse engineering Go binaries is challenging
  - Huge file size
  - Unusual string handling
  - No symbol names due to stripping
- Ghidra open-source development is in early stage compared to other tools
  - Only a few open-source scripts are available, solving only parts of the problem

Goal:

- Making reverse engineering Go binaries with Ghidra easier

Steps:

- Understand Go and the differences from usual languages
- Get familiar with Ghidra’s features (In this research we used Ghidra 9.1 and 9.2.3 versions.)
- Create our own scripts: https://github.com/getCUJO/ThreatIntel

Golang

Introduction

- Go (also called Golang) is an open source programming language
- Designed by Google in 2007
- Made available to the public in 2012
- Current version is Go 1.16 (in this research we used Go versions up to 1.15)
- https://golang.org/

- Go comes out top of the languages most developers want to learn[1]
- Advantages:
  - Simple and clear documentation
  - Easy to learn, ease of coding
  - Compiled language (faster than Python)
  - Cross compiling (Windows, Linux, macOS)
  - Scalability and concurrency
  - Garbage collection – automatic memory management

[1]: https://www.zdnet.com/article/developers-say-googles-go-is-most-sought-after-programming-language-of-2020/

Static linking

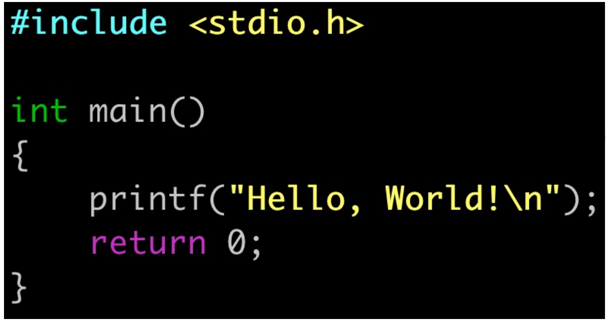
Big Bad Binaries

- Go binaries are statically linked by default
- All the necessary libraries are included in the executable image
- No dependency issues
- Large size
  - Difficult malware distribution
  - Anti – virus products have difficulty to detect
  - Reverse engineering can be more time consuming

Hello World - Unstripped

C vs Go

- C



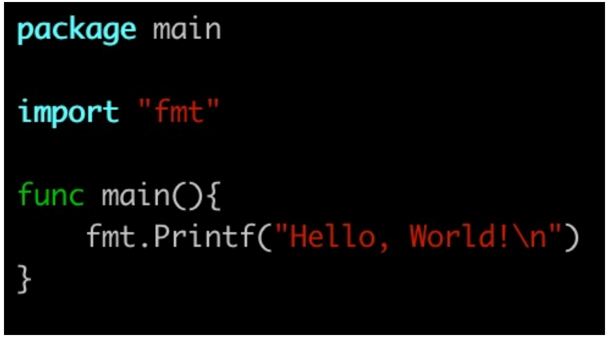
```c
#include <stdio.h>

int main()
{
    printf("Hello, World!\n");
    return 0;
}
```

gcc -o world_c world.c

ELF 64-bit LSB shared object,
x86-64, version 1 (SYSV),
dynamically linked,
not stripped

size: 16,3 kB

- Go



```go
package main

import "fmt"

func main(){
    fmt.Printf("Hello, World!\n")
}
```

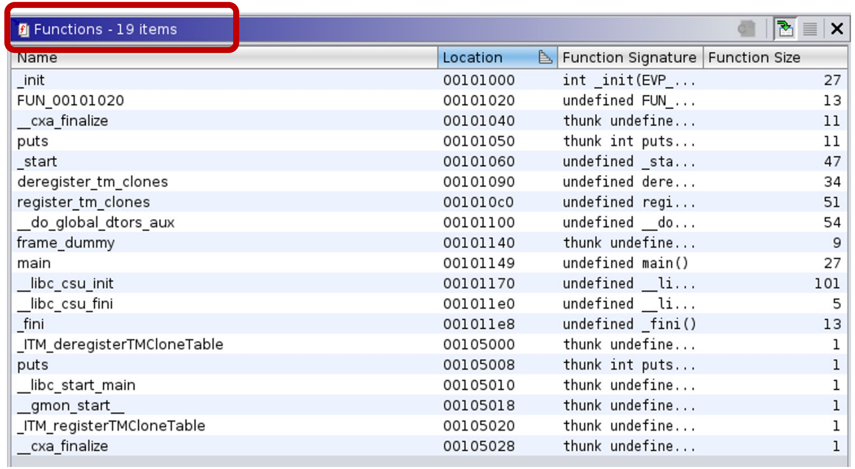
go build -o world_go world.go

ELF 64-bit LSB executable,
x86-64, version 1 (SYSV),
statically linked,
not stripped

size: 2,0 MB

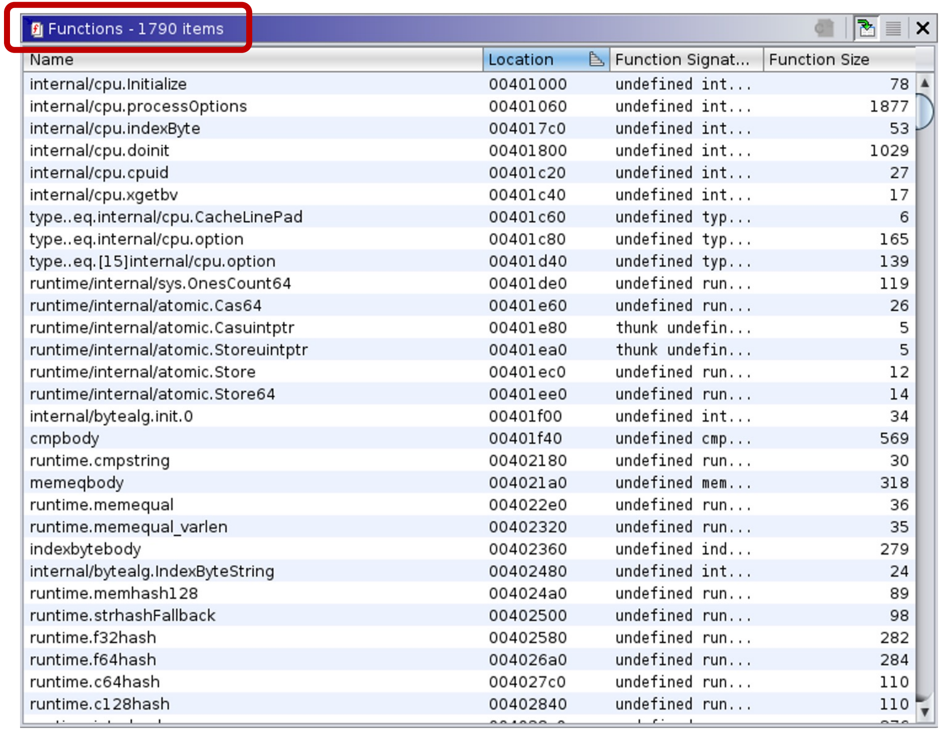
Hello World in Ghidra

C vs Go



Functions - 19 items

Name	Location	Function Signature	Function Size
_init	00101000	int _init(EVP_...	27
FUN_00101020	00101020	undefined FUN_...	13
__cxa_finalize	00101040	thunk undefine...	11
puts	00101050	thunk int puts...	11
_start	00101060	undefined _sta...	47
deregister_tm_clones	00101090	undefined dere...	34
register_tm_clones	001010c0	undefined regi...	51
__do_global_dtors_aux	00101100	undefined __do...	54
frame_dummy	00101140	thunk undefine...	9
main	00101149	undefined main()	27
__libc_csu_init	00101170	undefined __li...	101
__libc_csu_fini	001011e0	undefined __li...	5
_fini	001011e8	undefined _fini()	13
_ITM_deregisterTMCloneTable	00105000	thunk undefine...	1
puts	00105008	thunk int puts...	1
__libc_start_main	00105010	thunk undefine...	1
__gmon_start__	00105018	thunk undefine...	1
_ITM_registerTMCloneTable	00105020	thunk undefine...	1
__cxa_finalize	00105028	thunk undefine...	1



Functions - 1790 items

Name	Location	Function Signat...	Function Size
internal/cpu.Initialize	00401000	undefined int...	78
internal/cpu.processOptions	00401060	undefined int...	1877
internal/cpu.indexByte	004017c0	undefined int...	53
internal/cpu.doinit	00401800	undefined int...	1029
internal/cpu.cpuid	00401c20	undefined int...	27
internal/cpu.xgetbv	00401c40	undefined int...	17
type..eq.internal/cpu.CacheLinePad	00401c60	undefined typ...	6
type..eq.internal/cpu.option	00401c80	undefined typ...	165
type..eq.[15]internal/cpu.option	00401d40	undefined typ...	139
runtime/internal/sys.OnesCount64	00401de0	undefined run...	119
runtime/internal/atomic.Cas64	00401e60	undefined run...	26
runtime/internal/atomic.Casuintptr	00401e80	thunk undefin...	5
runtime/internal/atomic.Storeuintptr	00401ea0	thunk undefin...	5
runtime/internal/atomic.Store	00401ec0	undefined run...	12
runtime/internal/atomic.Store64	00401ee0	undefined run...	14
internal/bytealg.init.0	00401f00	undefined int...	34
cmpbody	00401f40	undefined cmp...	569
runtime.cmpstring	00402180	undefined run...	30
memeqbody	004021a0	undefined mem...	318
runtime.memequal	004022e0	undefined run...	36
runtime.memequal_varlen	00402320	undefined run...	35
indexbytebody	00402360	undefined ind...	279
internal/bytealg.IndexByteString	00402480	undefined int...	24
runtime.memhash128	004024a0	undefined run...	89
runtime.strhashFallback	00402500	undefined run...	98
runtime.f32hash	00402580	undefined run...	282
runtime.f64hash	004026a0	undefined run...	284
runtime.c64hash	004027c0	undefined run...	110
runtime.c128hash	00402840	undefined run...	110

19 functions vs 1790 functions

Binaries: world_c, world_go

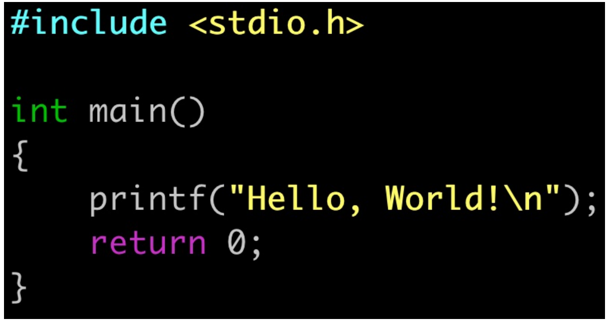
Stripped Binaries

- Discard debugging symbols
- Reduced size
- No names for routines and variables
- More difficult debugging and reverse engineering
- Malware files are usually stripped

Hello World - Stripped

C vs Go

- C



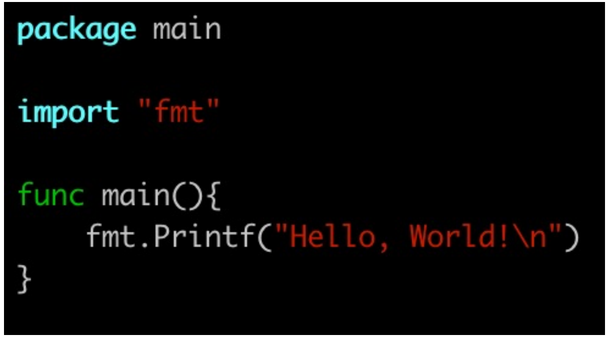
```c
#include <stdio.h>

int main()
{
    printf("Hello, World!\n");
    return 0;
}
```

gcc -o world_c_strip **-s** world.c

ELF 64-bit LSB shared object,
x86-64, version 1 (SYSV),
dynamically linked,
stripped

size: 14,1 kB

- Go



```go
package main

import "fmt"

func main(){
    fmt.Printf("Hello, World!\n")
}
```

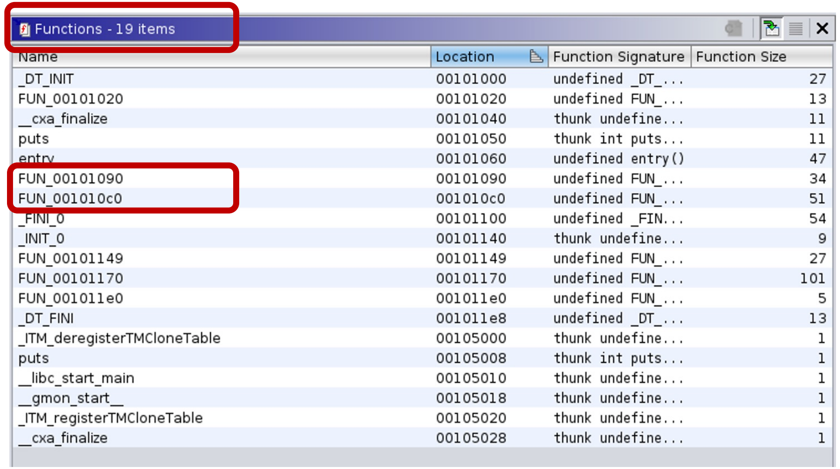
go build -o world_go_strip **–ldflags “-s”** world.go

ELF 64-bit LSB executable,
x86-64, version 1 (SYSV),
statically linked,
stripped

size: 1,3 MB

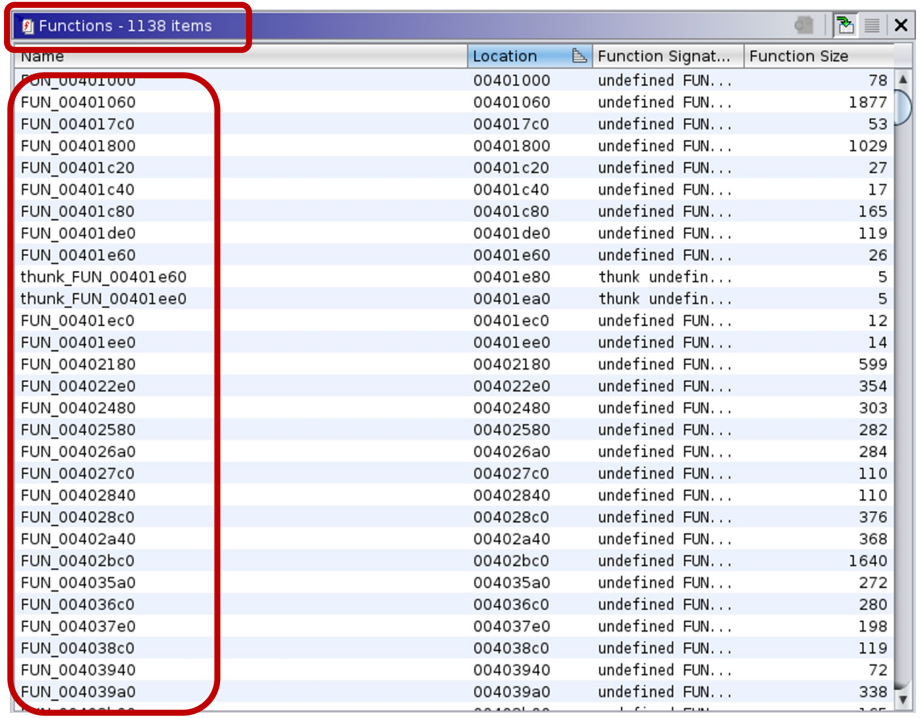
Hello World Stripped in Ghidra

C vs Go



Functions - 19 items

Name	Location	Function Signature	Function Size
_DT_INIT	00101000	undefined _DT_...	27
FUN_00101020	00101020	undefined FUN_...	13
__cxa_finalize	00101040	thunk undefine...	11
puts	00101050	thunk int puts...	11
entry	00101060	undefined entry()	47
FUN_00101090	00101090	undefined FUN_...	34
FUN_001010c0	001010c0	undefined FUN_...	51
_FINI_0	00101100	undefined _FIN...	54
_INIT_0	00101140	thunk undefine...	9
FUN_00101149	00101149	undefined FUN_...	27
FUN_00101170	00101170	undefined FUN_...	101
FUN_001011e0	001011e0	undefined FUN_...	5
_DT_FINI	001011e8	undefined _DT_...	13
_ITM_deregisterTMCloneTable	00105000	thunk undefine...	1
puts	00105008	thunk int puts...	1
__libc_start_main	00105010	thunk undefine...	1
__gmon_start__	00105018	thunk undefine...	1
_ITM_registerTMCloneTable	00105020	thunk undefine...	1
__cxa_finalize	00105028	thunk undefine...	1



Functions - 1138 items

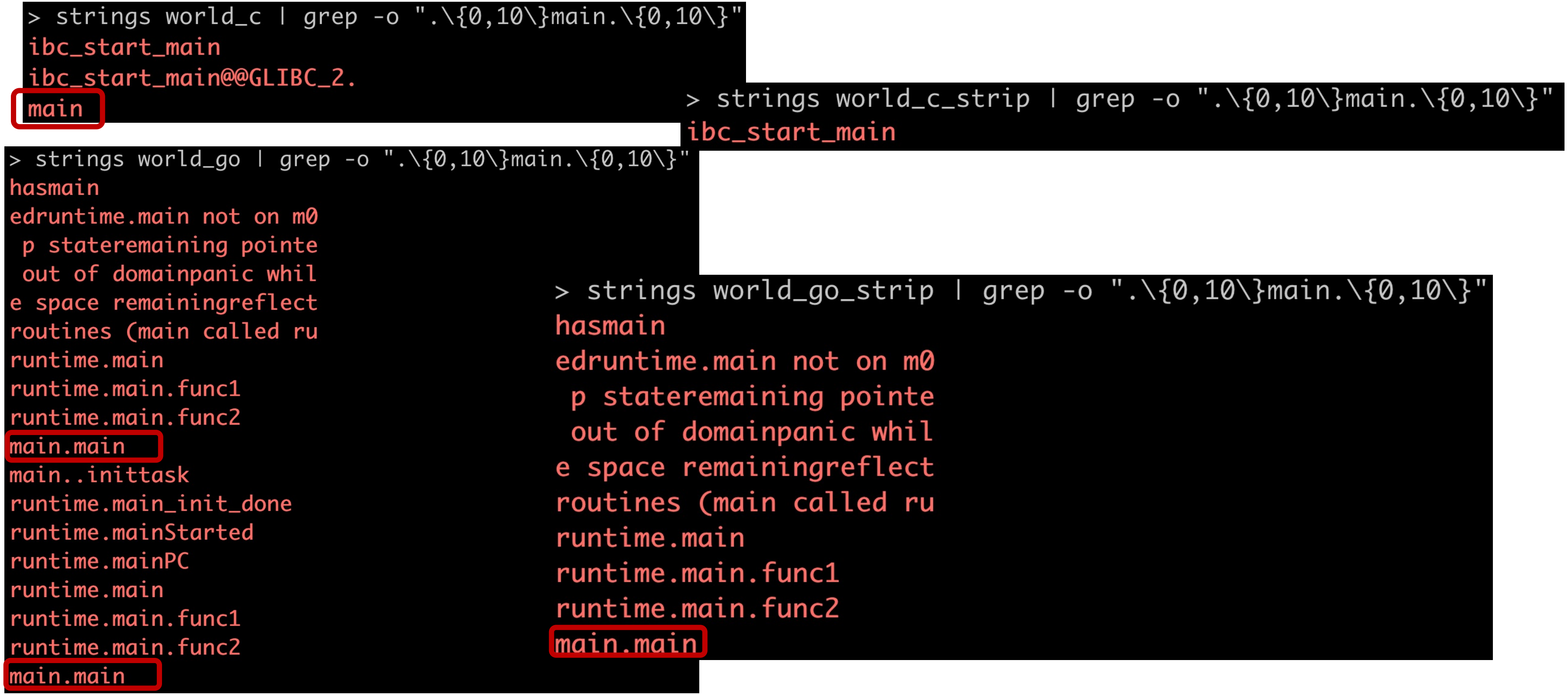
Name	Location	Function Signat...	Function Size
FUN_00401000	00401000	undefined FUN...	78
FUN_00401060	00401060	undefined FUN...	1877
FUN_004017c0	004017c0	undefined FUN...	53
FUN_00401800	00401800	undefined FUN...	1029
FUN_00401c20	00401c20	undefined FUN...	27
FUN_00401c40	00401c40	undefined FUN...	17
FUN_00401c80	00401c80	undefined FUN...	165
FUN_00401de0	00401de0	undefined FUN...	119
FUN_00401e60	00401e60	undefined FUN...	26
thunk_FUN_00401e60	00401e80	thunk undefin...	5
thunk_FUN_00401ee0	00401ea0	thunk undefin...	5
FUN_00401ec0	00401ec0	undefined FUN...	12
FUN_00401ee0	00401ee0	undefined FUN...	14
FUN_00402180	00402180	undefined FUN...	599
FUN_004022e0	004022e0	undefined FUN...	354
FUN_00402480	00402480	undefined FUN...	303
FUN_00402580	00402580	undefined FUN...	282
FUN_004026a0	004026a0	undefined FUN...	284
FUN_004027c0	004027c0	undefined FUN...	110
FUN_00402840	00402840	undefined FUN...	110
FUN_004028c0	004028c0	undefined FUN...	376
FUN_00402a40	00402a40	undefined FUN...	368
FUN_00402bc0	00402bc0	undefined FUN...	1640
FUN_004035a0	004035a0	undefined FUN...	272
FUN_004036c0	004036c0	undefined FUN...	280
FUN_004037e0	004037e0	undefined FUN...	198
FUN_004038c0	004038c0	undefined FUN...	119
FUN_00403940	00403940	undefined FUN...	72
FUN_004039a0	004039a0	undefined FUN...	338

19 functions vs 1138 functions

Binaries: world_c_strip, world_go_strip

Recover function names

strings



```
> strings world_c | grep -o ".\{0,10\}main.\{0,10\}"
ibc_start_main
ibc_start_main@@GLIBC_2.
main
```

```
> strings world_c_strip | grep -o ".\{0,10\}main.\{0,10\}"
ibc_start_main
```

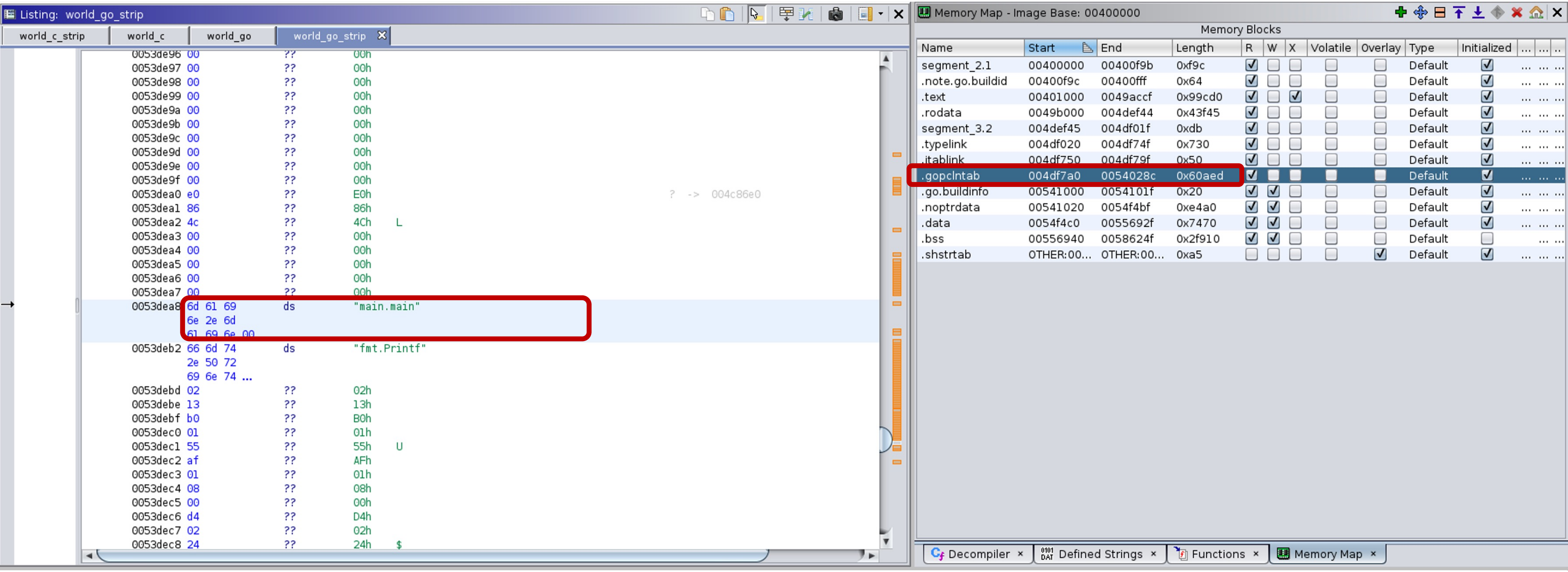
```
> strings world_go | grep -o ".\{0,10\}main.\{0,10\}"
hasmain
edruntime.main not on m0
 p stateremaining pointe
 out of domainpanic whil
e space remainingreflect
routines (main called ru
runtime.main
runtime.main.func1
runtime.main.func2
main.main
main..inittask
runtime.main_init_done
runtime.mainStarted
runtime.mainPC
runtime.main
runtime.main.func1
runtime.main.func2
main.main
```

```
> strings world_go_strip | grep -o ".\{0,10\}main.\{0,10\}"
hasmain
edruntime.main not on m0
 p stateremaining pointe
 out of domainpanic whil
e space remainingreflect
routines (main called ru
runtime.main
runtime.main.func1
runtime.main.func2
main.main
```

Binaries: world_c, world_go, world_c_strip, world_go_strip

Recover function names

pclntab



```
0053de96 00         ??    00h
0053de97 00         ??    00h
0053de98 00         ??    00h
0053de99 00         ??    00h
0053de9a 00         ??    00h
0053de9b 00         ??    00h
0053de9c 00         ??    00h
0053de9d 00         ??    00h
0053de9e 00         ??    00h
0053de9f 00         ??    00h
0053dea0 e0         ??    E0h                    ?  ->  004c86e0
0053dea1 86         ??    86h
0053dea2 4c         ??    4Ch    L
0053dea3 00         ??    00h
0053dea4 00         ??    00h
0053dea5 00         ??    00h
0053dea6 00         ??    00h
0053dea7 00         ??    00h
0053dea8 6d 61 69   ds    "main.main"
         6e 2e 6d
         61 69 6e 00
0053deb2 66 6d 74   ds    "fmt.Printf"
         2e 50 72
         69 6e 74 ...
0053debd 02         ??    02h
0053debe 13         ??    13h
0053debf b0         ??    B0h
0053dec0 01         ??    01h
0053dec1 55         ??    55h    U
0053dec2 af         ??    AFh
0053dec3 01         ??    01h
0053dec4 08         ??    08h
0053dec5 00         ??    00h
0053dec6 d4         ??    D4h
0053dec7 02         ??    02h
0053dec8 24         ??    24h    $
```

Memory Map - Image Base: 00400000

Memory Blocks

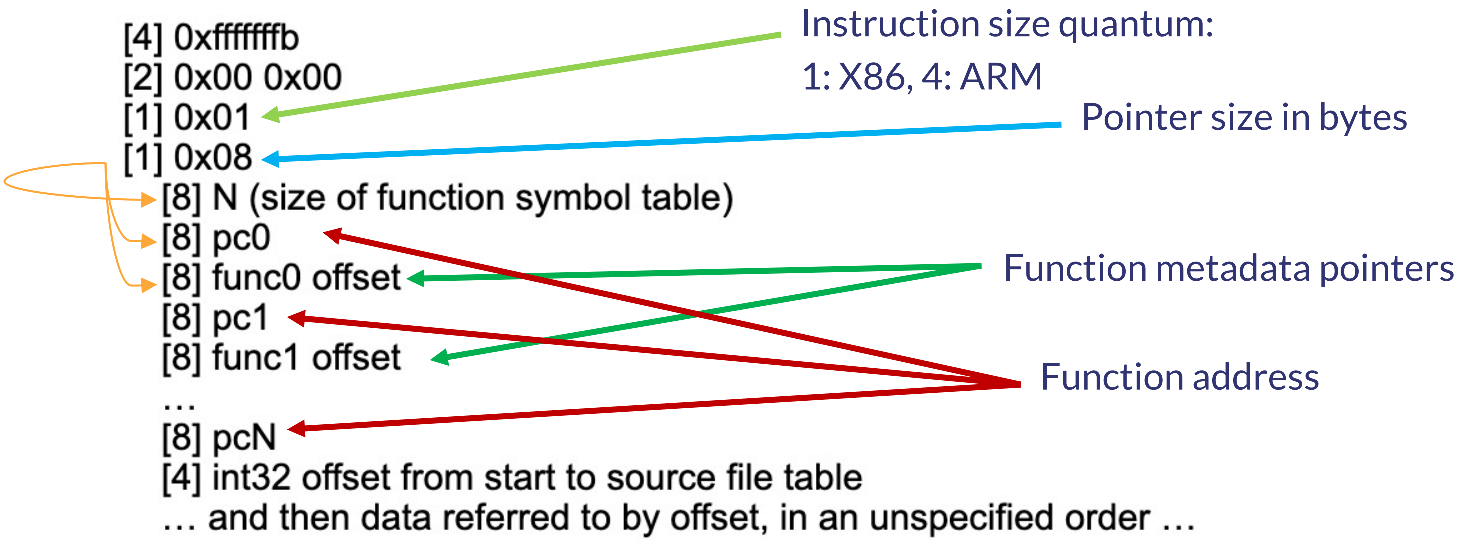
Name	Start	End	Length	R	W	X	Volatile	Overlay	Type	Initialized	...	...	...
segment_2.1	00400000	00400f9b	0xf9c	☑	☐	☐	☐	☐	Default	☑	...	...	...
.note.go.buildid	00400f9c	00400fff	0x64	☑	☐	☐	☐	☐	Default	☑	...	...	...
.text	00401000	0049accf	0x99cd0	☑	☐	☑	☐	☐	Default	☑	...	...	...
.rodata	0049b000	004def44	0x43f45	☑	☐	☐	☐	☐	Default	☑	...	...	...
segment_3.2	004def45	004df01f	0xdb	☑	☐	☐	☐	☐	Default	☑	...	...	...
.typelink	004df020	004df74f	0x730	☑	☐	☐	☐	☐	Default	☑	...	...	...
.itablink	004df750	004df79f	0x50	☑	☐	☐	☐	☐	Default	☑	...	...	...
.gopclntab	004df7a0	0054028c	0x60aed	☑	☐	☐	☐	☐	Default	☑	...	...	...
.go.buildinfo	00541000	0054101f	0x20	☑	☑	☐	☐	☐	Default	☑	...	...	...
.noptrdata	00541020	0054f4bf	0xe4a0	☑	☑	☐	☐	☐	Default	☑	...	...	...
.data	0054f4c0	0055692f	0x7470	☑	☑	☐	☐	☐	Default	☑	...	...	...
.bss	00556940	0058624f	0x2f910	☑	☑	☐	☐	☐	Default	☐		...	...
.shstrtab	OTHER:00...	OTHER:00...	0xa5	☐	☐	☐	☐	☑	Default	☑	...	...	...

Binary: world_go_strip

Recover function names

pclntab

- Detailed documentation of pclntab[1] is available



```
[4] 0xfffffffb
[2] 0x00 0x00
[1] 0x01
[1] 0x08
    [8] N (size of function symbol table)
    [8] pc0
    [8] func0 offset
    [8] pc1
    [8] func1 offset
    …
    [8] pcN
    [4] int32 offset from start to source file table
    … and then data referred to by offset, in an unspecified order …
```

Instruction size quantum:
1: X86, 4: ARM

Pointer size in bytes

Function metadata pointers

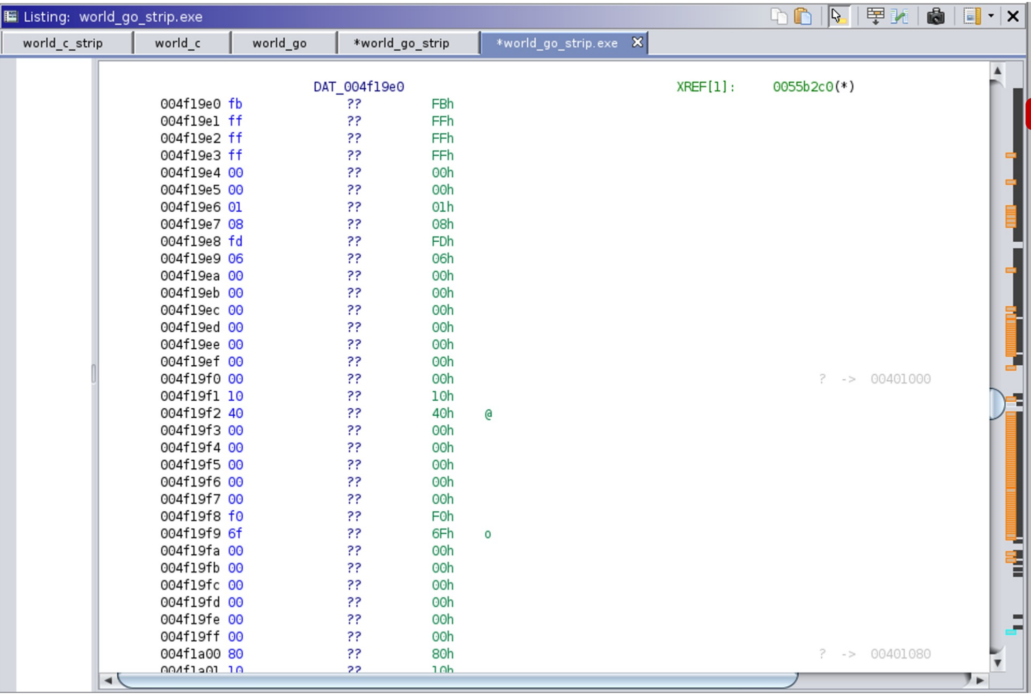
Function address

[1] https://docs.google.com/document/d/1lyPIbmsYbXnpNj57a261hgOYVpNRcgydurVQIyZOz_o/pub

Recover function names

pclntab in Windows

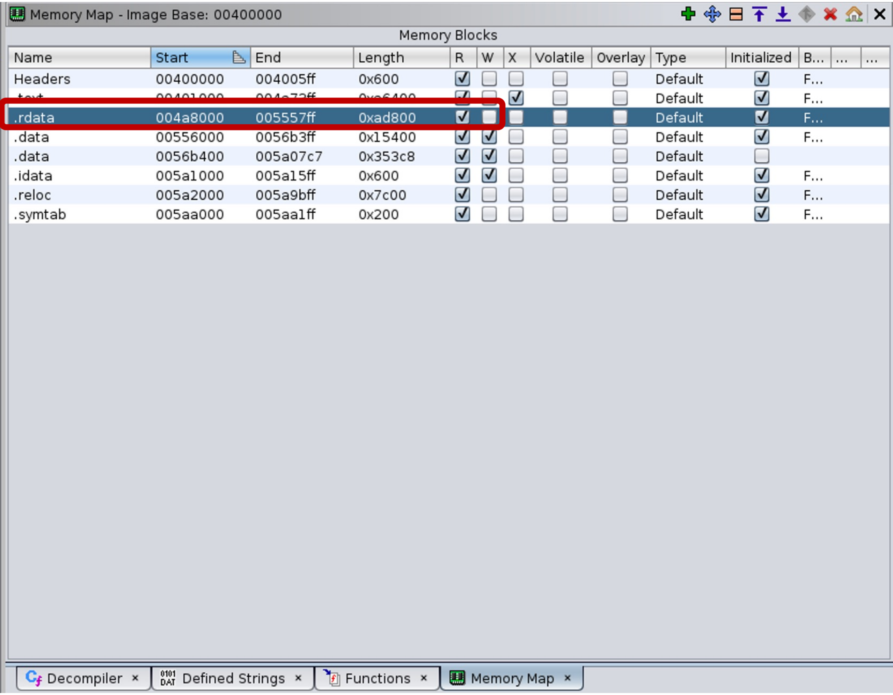
- Not a separate section -> Look for the structure



Listing: world_go_strip.exe

world_c_strip | world_c | world_go | *world_go_strip | *world_go_strip.exe

```
                         DAT_004f19e0                              XREF[1]:     0055b2c0(*)
        004f19e0 fb           ??         FBh
        004f19e1 ff           ??         FFh
        004f19e2 ff           ??         FFh
        004f19e3 ff           ??         FFh
        004f19e4 00           ??         00h
        004f19e5 00           ??         00h
        004f19e6 01           ??         01h
        004f19e7 08           ??         08h
        004f19e8 fd           ??         FDh
        004f19e9 06           ??         06h
        004f19ea 00           ??         00h
        004f19eb 00           ??         00h
        004f19ec 00           ??         00h
        004f19ed 00           ??         00h
        004f19ee 00           ??         00h
        004f19ef 00           ??         00h
        004f19f0 00           ??         00h                                    ?  ->  00401000
        004f19f1 10           ??         10h
        004f19f2 40           ??         40h    @
        004f19f3 00           ??         00h
        004f19f4 00           ??         00h
        004f19f5 00           ??         00h
        004f19f6 00           ??         00h
        004f19f7 00           ??         00h
        004f19f8 f0           ??         F0h
        004f19f9 6f           ??         6Fh    o
        004f19fa 00           ??         00h
        004f19fb 00           ??         00h
        004f19fc 00           ??         00h
        004f19fd 00           ??         00h
        004f19fe 00           ??         00h
        004f19ff 00           ??         00h
        004f1a00 80           ??         80h                                    ?  ->  00401080
        004f1a01 10           ??         10h
```



Memory Map - Image Base: 00400000

Memory Blocks

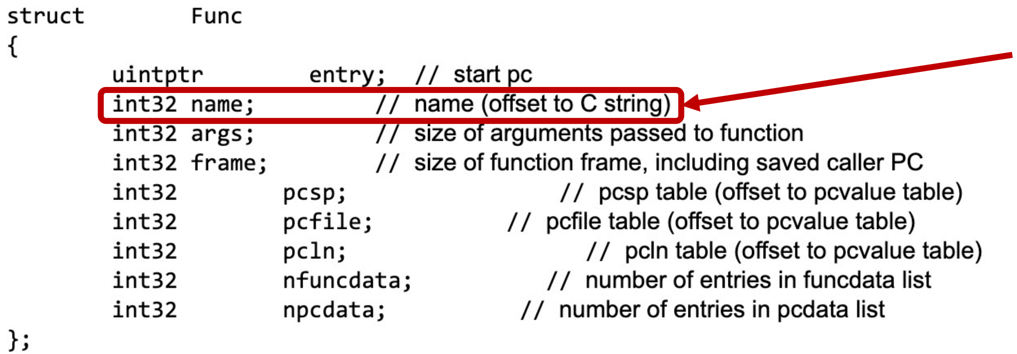
Name	Start	End	Length	R	W	X	Volatile	Overlay	Type	Initialized	B...	...	...
Headers	00400000	004005ff	0x600	☑	☐	☐	☐	☐	Default	☑	F...		
.text	00401000	004a73ff	0xa6400	☑	☐	☑	☐	☐	Default	☑	F...		
.rdata	004a8000	005557ff	0xad800	☑	☐	☐	☐	☐	Default	☑	F...		
.data	00556000	0056b3ff	0x15400	☑	☑	☐	☐	☐	Default	☑	F...		
.data	0056b400	005a07c7	0x353c8	☑	☑	☐	☐	☐	Default	☐			
.idata	005a1000	005a15ff	0x600	☑	☑	☐	☐	☐	Default	☑	F...		
.reloc	005a2000	005a9bff	0x7c00	☑	☐	☐	☐	☐	Default	☑	F...		
.symtab	005aa000	005aa1ff	0x200	☑	☐	☐	☐	☐	Default	☑	F...		

Binary: world_go_strip.exe

Recover function names

pclntab

- Function metadata



```
struct        Func
{
        uintptr        entry;   // start pc
        int32 name;          // name (offset to C string)
        int32 args;          // size of arguments passed to function
        int32 frame;         // size of function frame, including saved caller PC
        int32       pcsp;                 // pcsp table (offset to pcvalue table)
        int32       pcfile;           // pcfile table (offset to pcvalue table)
        int32       pcln;                  // pcln table (offset to pcvalue table)
        int32       nfuncdata;            // number of entries in funcdata list
        int32       npcdata;            // number of entries in pcdata list
};
```

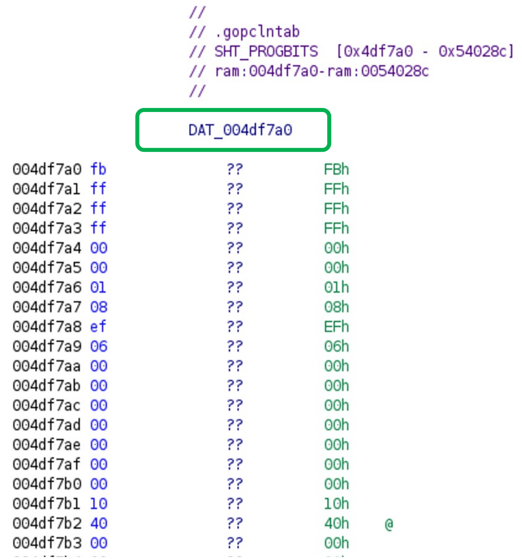
Function name offset

Recover function names

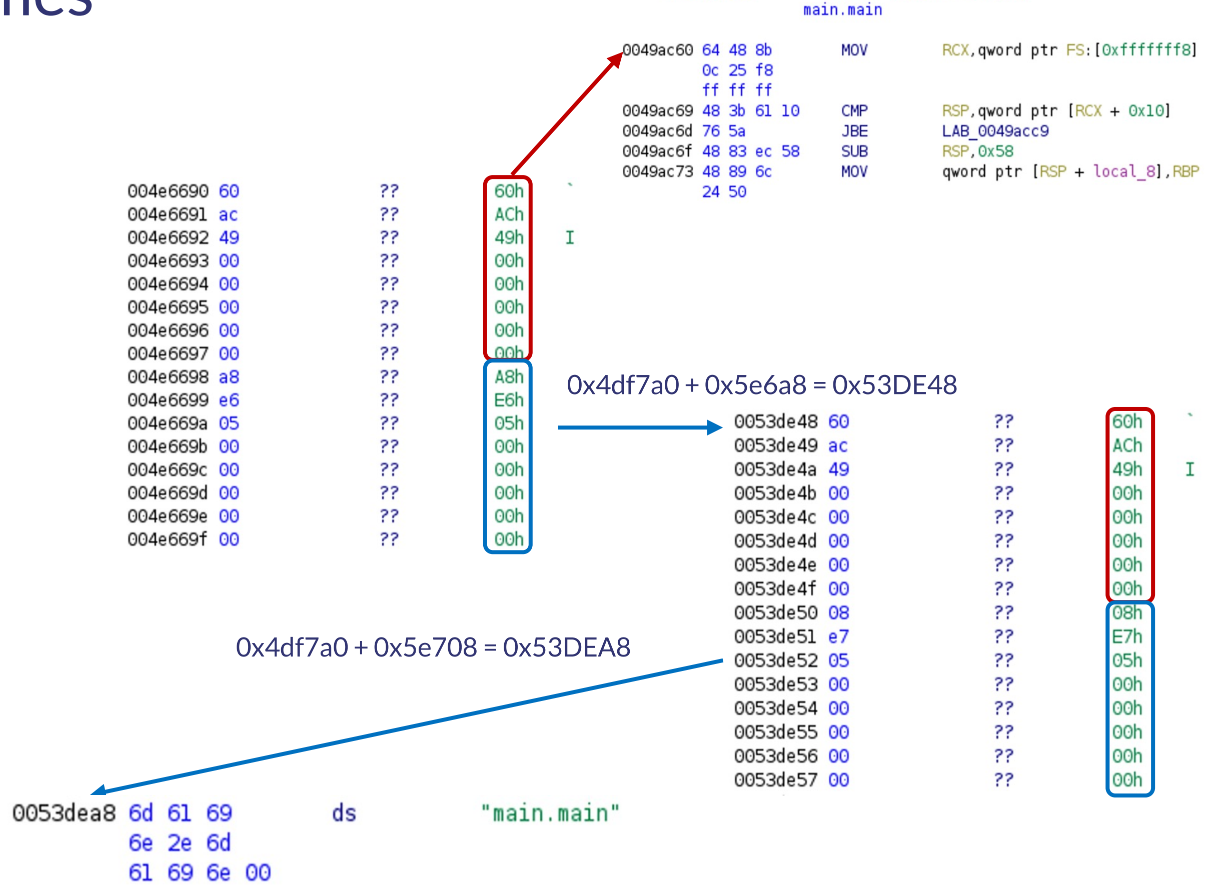
Idea

Function name recovery steps:

- Locate pclntab structure
- Extract function addresses
- Find function name offsets



```
                    //
                    // .gopclntab
                    // SHT_PROGBITS  [0x4df7a0 - 0x54028c]
                    // ram:004df7a0-ram:0054028c
                    //
                 DAT_004df7a0
004df7a0 fb          ??       FBh
004df7a1 ff          ??       FFh
004df7a2 ff          ??       FFh
004df7a3 ff          ??       FFh
004df7a4 00          ??       00h
004df7a5 00          ??       00h
004df7a6 01          ??       01h
004df7a7 08          ??       08h
004df7a8 ef          ??       EFh
004df7a9 06          ??       06h
004df7aa 00          ??       00h
004df7ab 00          ??       00h
004df7ac 00          ??       00h
004df7ad 00          ??       00h
004df7ae 00          ??       00h
004df7af 00          ??       00h
004df7b0 00          ??       00h
004df7b1 10          ??       10h
004df7b2 40          ??       40h    @
004df7b3 00          ??       00h
```



```
                         main.main
0049ac60 64 48 8b        MOV     RCX,qword ptr FS:[0xfffffff8]
         0c 25 f8
         ff ff ff
0049ac69 48 3b 61 10     CMP     RSP,qword ptr [RCX + 0x10]
0049ac6d 76 5a           JBE     LAB_0049acc9
0049ac6f 48 83 ec 58     SUB     RSP,0x58
0049ac73 48 89 6c        MOV     qword ptr [RSP + local_8],RBP
         24 50
```

```
004e6690 60          ??       60h    `
004e6691 ac          ??       ACh
004e6692 49          ??       49h    I
004e6693 00          ??       00h
004e6694 00          ??       00h
004e6695 00          ??       00h
004e6696 00          ??       00h
004e6697 00          ??       00h
004e6698 a8          ??       A8h
004e6699 e6          ??       E6h
004e669a 05          ??       05h
004e669b 00          ??       00h
004e669c 00          ??       00h
004e669d 00          ??       00h
004e669e 00          ??       00h
004e669f 00          ??       00h
```

0x4df7a0 + 0x5e6a8 = 0x53DE48

```
0053de48 60          ??       60h    `
0053de49 ac          ??       ACh
0053de4a 49          ??       49h    I
0053de4b 00          ??       00h
0053de4c 00          ??       00h
0053de4d 00          ??       00h
0053de4e 00          ??       00h
0053de4f 00          ??       00h
0053de50 08          ??       08h
0053de51 e7          ??       E7h
0053de52 05          ??       05h
0053de53 00          ??       00h
0053de54 00          ??       00h
0053de55 00          ??       00h
0053de56 00          ??       00h
0053de57 00          ??       00h
```

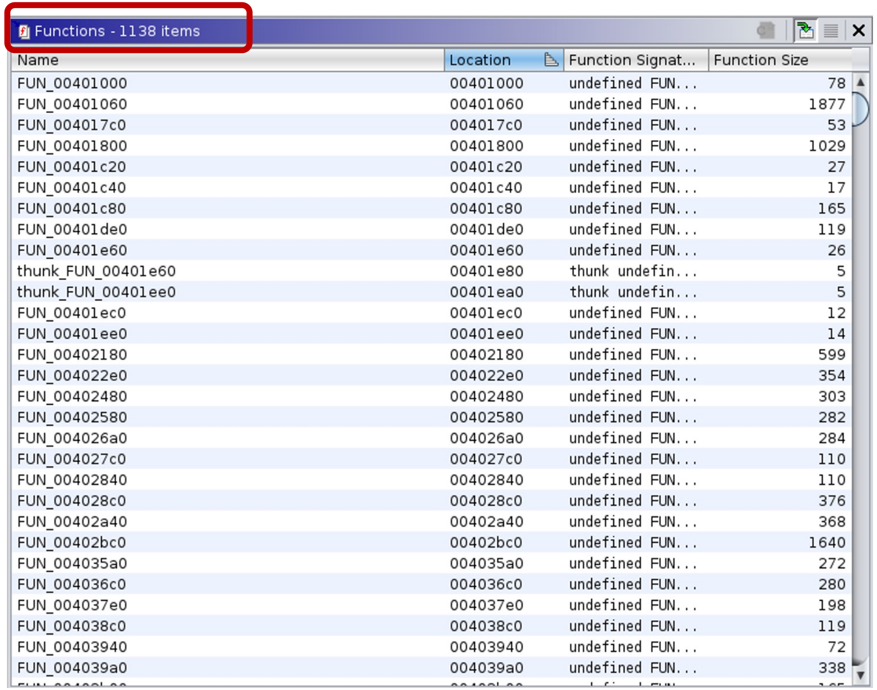
0x4df7a0 + 0x5e708 = 0x53DEA8

```
0053dea8 6d 61 69     ds     "main.main"
         6e 2e 6d
         61 69 6e 00
```

Binary: world_go_strip

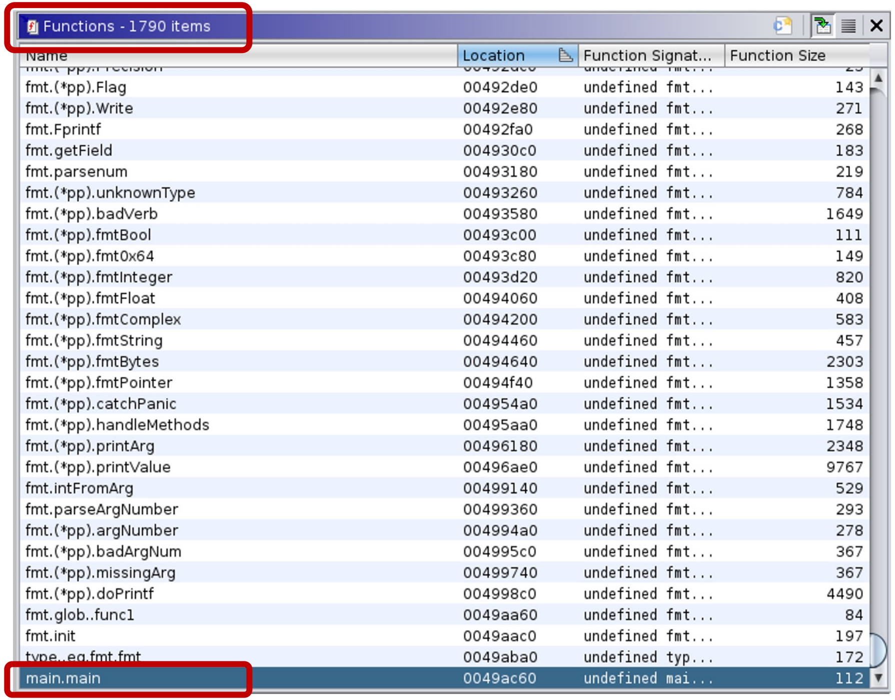
Recover function names

Executing our script



Functions - 1138 items

Name	Location	Function Signat...	Function Size
FUN_00401000	00401000	undefined FUN...	78
FUN_00401060	00401060	undefined FUN...	1877
FUN_004017c0	004017c0	undefined FUN...	53
FUN_00401800	00401800	undefined FUN...	1029
FUN_00401c20	00401c20	undefined FUN...	27
FUN_00401c40	00401c40	undefined FUN...	17
FUN_00401c80	00401c80	undefined FUN...	165
FUN_00401de0	00401de0	undefined FUN...	119
FUN_00401e60	00401e60	undefined FUN...	26
thunk_FUN_00401e60	00401e80	thunk undefin...	5
thunk_FUN_00401ee0	00401ea0	thunk undefin...	5
FUN_00401ec0	00401ec0	undefined FUN...	12
FUN_00401ee0	00401ee0	undefined FUN...	14
FUN_00402180	00402180	undefined FUN...	599
FUN_004022e0	004022e0	undefined FUN...	354
FUN_00402480	00402480	undefined FUN...	303
FUN_00402580	00402580	undefined FUN...	282
FUN_004026a0	004026a0	undefined FUN...	284
FUN_004027c0	004027c0	undefined FUN...	110
FUN_00402840	00402840	undefined FUN...	110
FUN_004028c0	004028c0	undefined FUN...	376
FUN_00402a40	00402a40	undefined FUN...	368
FUN_00402bc0	00402bc0	undefined FUN...	1640
FUN_004035a0	004035a0	undefined FUN...	272
FUN_004036c0	004036c0	undefined FUN...	280
FUN_004037e0	004037e0	undefined FUN...	198
FUN_004038c0	004038c0	undefined FUN...	119
FUN_00403940	00403940	undefined FUN...	72
FUN_004039a0	004039a0	undefined FUN...	338



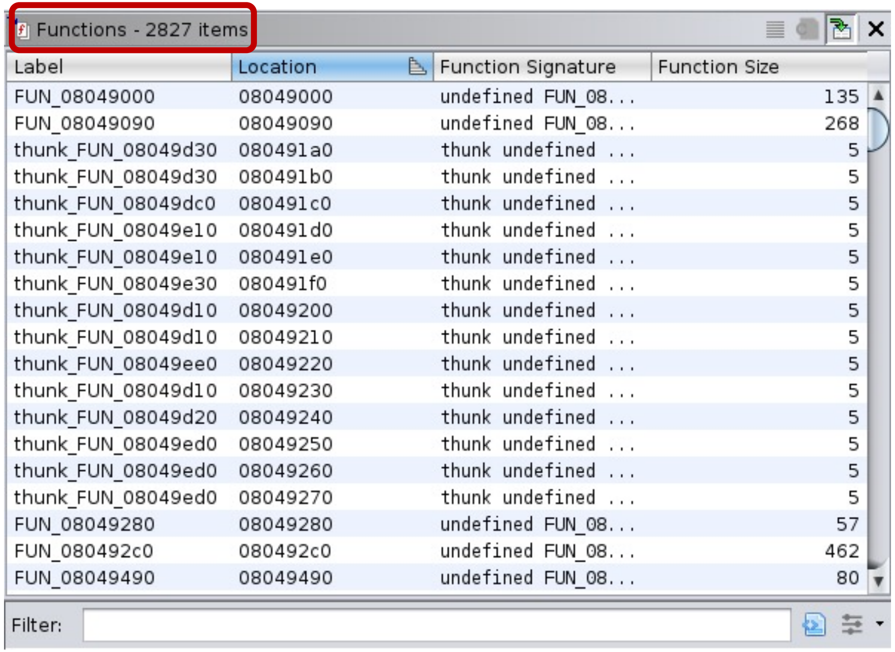
Functions - 1790 items

Name	Location	Function Signat...	Function Size
fmt.(*pp).Flag	00492de0	undefined fmt...	143
fmt.(*pp).Write	00492e80	undefined fmt...	271
fmt.Fprintf	00492fa0	undefined fmt...	268
fmt.getField	004930c0	undefined fmt...	183
fmt.parsenum	00493180	undefined fmt...	219
fmt.(*pp).unknownType	00493260	undefined fmt...	784
fmt.(*pp).badVerb	00493580	undefined fmt...	1649
fmt.(*pp).fmtBool	00493c00	undefined fmt...	111
fmt.(*pp).fmt0x64	00493c80	undefined fmt...	149
fmt.(*pp).fmtInteger	00493d20	undefined fmt...	820
fmt.(*pp).fmtFloat	00494060	undefined fmt...	408
fmt.(*pp).fmtComplex	00494200	undefined fmt...	583
fmt.(*pp).fmtString	00494460	undefined fmt...	457
fmt.(*pp).fmtBytes	00494640	undefined fmt...	2303
fmt.(*pp).fmtPointer	00494f40	undefined fmt...	1358
fmt.(*pp).catchPanic	004954a0	undefined fmt...	1534
fmt.(*pp).handleMethods	00495aa0	undefined fmt...	1748
fmt.(*pp).printArg	00496180	undefined fmt...	2348
fmt.(*pp).printValue	00496ae0	undefined fmt...	9767
fmt.intFromArg	00499140	undefined fmt...	529
fmt.parseArgNumber	00499360	undefined fmt...	293
fmt.(*pp).argNumber	004994a0	undefined fmt...	278
fmt.(*pp).badArgNum	004995c0	undefined fmt...	367
fmt.(*pp).missingArg	00499740	undefined fmt...	367
fmt.(*pp).doPrintf	004998c0	undefined fmt...	4490
fmt.glob..func1	0049aa60	undefined fmt...	84
fmt.init	0049aac0	undefined fmt...	197
type..eq.fmt.fmt	0049aba0	undefined typ...	172
main.main	0049ac60	undefined mai...	112

Binary: world_go_strip

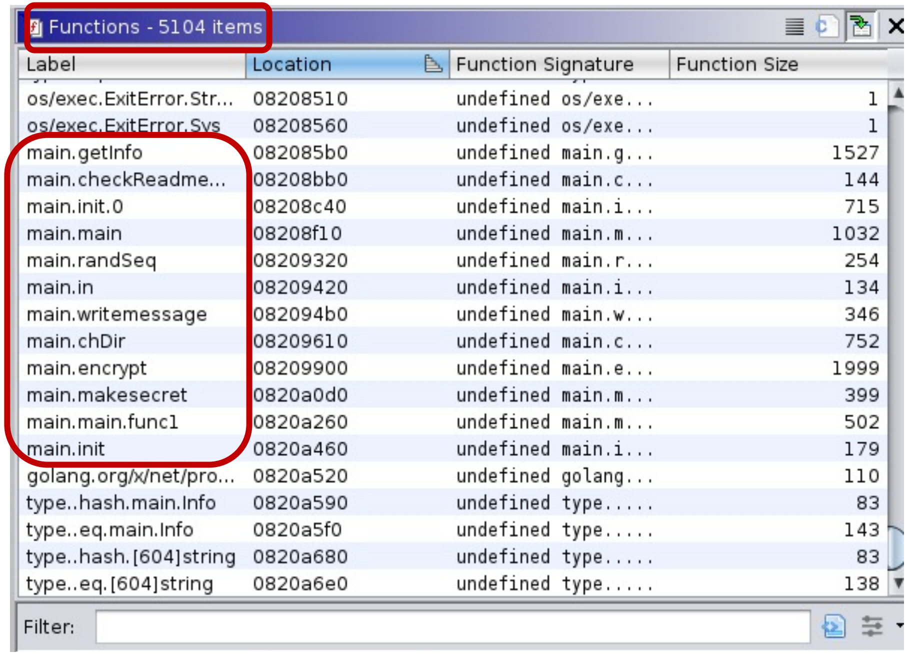
Recover function names

Real world example – eCh0raix



Functions - 2827 items

Label	Location	Function Signature	Function Size
FUN_08049000	08049000	undefined FUN_08...	135
FUN_08049090	08049090	undefined FUN_08...	268
thunk_FUN_08049d30	080491a0	thunk undefined ...	5
thunk_FUN_08049d30	080491b0	thunk undefined ...	5
thunk_FUN_08049dc0	080491c0	thunk undefined ...	5
thunk_FUN_08049e10	080491d0	thunk undefined ...	5
thunk_FUN_08049e10	080491e0	thunk undefined ...	5
thunk_FUN_08049e30	080491f0	thunk undefined ...	5
thunk_FUN_08049d10	08049200	thunk undefined ...	5
thunk_FUN_08049d10	08049210	thunk undefined ...	5
thunk_FUN_08049ee0	08049220	thunk undefined ...	5
thunk_FUN_08049d10	08049230	thunk undefined ...	5
thunk_FUN_08049d20	08049240	thunk undefined ...	5
thunk_FUN_08049ed0	08049250	thunk undefined ...	5
thunk_FUN_08049ed0	08049260	thunk undefined ...	5
thunk_FUN_08049ed0	08049270	thunk undefined ...	5
FUN_08049280	08049280	undefined FUN_08...	57
FUN_080492c0	080492c0	undefined FUN_08...	462
FUN_08049490	08049490	undefined FUN_08...	80



Functions - 5104 items

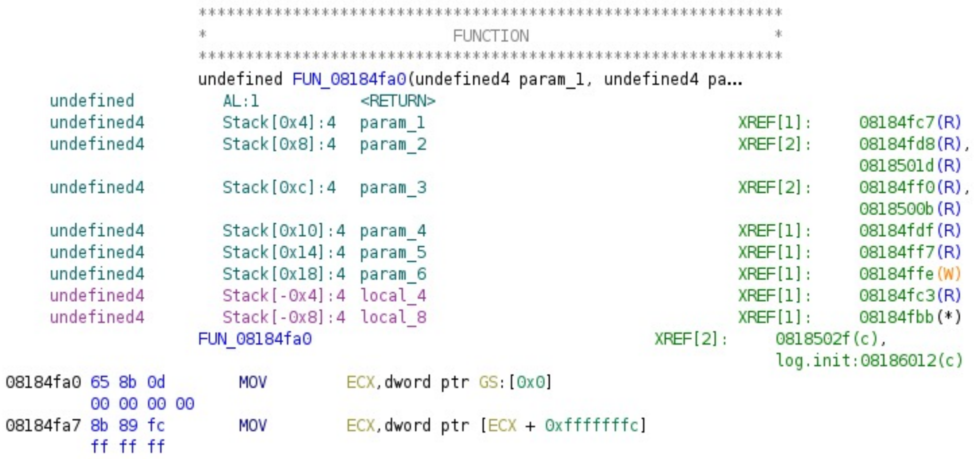
Label	Location	Function Signature	Function Size
os/exec.ExitError.Str...	08208510	undefined os/exe...	1
os/exec.ExitError.Sys	08208560	undefined os/exe...	1
main.getInfo	082085b0	undefined main.g...	1527
main.checkReadme...	08208bb0	undefined main.c...	144
main.init.0	08208c40	undefined main.i...	715
main.main	08208f10	undefined main.m...	1032
main.randSeq	08209320	undefined main.r...	254
main.in	08209420	undefined main.i...	134
main.writemessage	082094b0	undefined main.w...	346
main.chDir	08209610	undefined main.c...	752
main.encrypt	08209900	undefined main.e...	1999
main.makesecret	0820a0d0	undefined main.m...	399
main.main.func1	0820a260	undefined main.m...	502
main.init	0820a460	undefined main.i...	179
golang.org/x/net/pro...	0820a520	undefined golang...	110
type..hash.main.Info	0820a590	undefined type....	83
type..eq.main.Info	0820a5f0	undefined type....	143
type..hash.[604]string	0820a680	undefined type....	83
type..eq.[604]string	0820a6e0	undefined type....	138

Binary: eCh0raix – x86

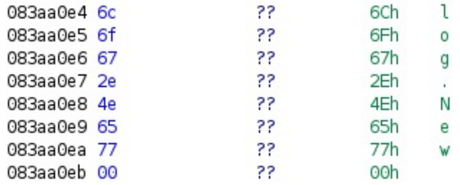
Recover function names

Challenges

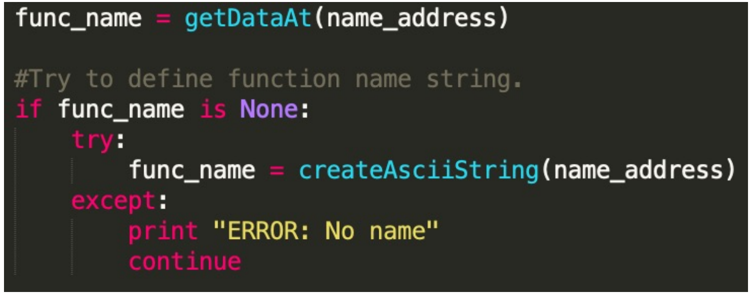
- Undefined function name strings



```
                        **************************************************************
                        *                          FUNCTION                          *
                        **************************************************************
                        undefined FUN_08184fa0(undefined4 param_1, undefined4 pa...
     undefined            AL:1           <RETURN>
     undefined4           Stack[0x4]:4   param_1                             XREF[1]:     08184fc7(R)
     undefined4           Stack[0x8]:4   param_2                             XREF[2]:     08184fd8(R),
                                                                                          0818501d(R)
     undefined4           Stack[0xc]:4   param_3                             XREF[2]:     08184ff0(R),
                                                                                          0818500b(R)
     undefined4           Stack[0x10]:4  param_4                             XREF[1]:     08184fdf(R)
     undefined4           Stack[0x14]:4  param_5                             XREF[1]:     08184ff7(R)
     undefined4           Stack[0x18]:4  param_6                             XREF[1]:     08184ffe(W)
     undefined4           Stack[-0x4]:4  local_4                             XREF[1]:     08184fc3(R)
     undefined4           Stack[-0x8]:4  local_8                             XREF[1]:     08184fbb(*)
                        FUN_08184fa0                                 XREF[2]:     0818502f(c),
                                                                                  log.init:08186012(c)
08184fa0 65 8b 0d         MOV         ECX,dword ptr GS:[0x0]
         00 00 00 00
08184fa7 8b 89 fc         MOV         ECX,dword ptr [ECX + 0xfffffffc]
         ff ff
```



```
083aa0e4 6c           ??         6Ch    l
083aa0e5 6f           ??         6Fh    o
083aa0e6 67           ??         67h    g
083aa0e7 2e           ??         2Eh    .
083aa0e8 4e           ??         4Eh    N
083aa0e9 65           ??         65h    e
083aa0ea 77           ??         77h    w
083aa0eb 00           ??         00h
```

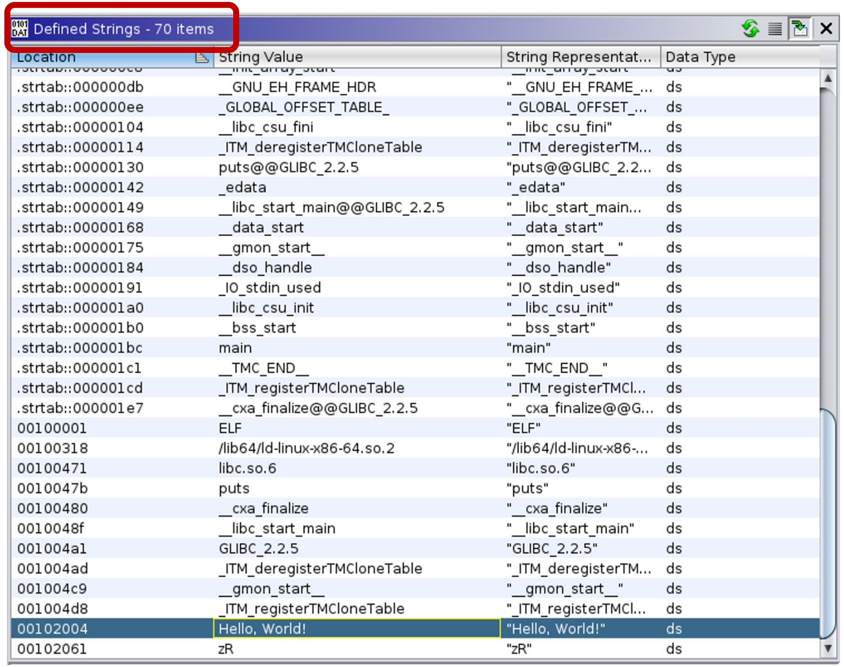


```
func_name = getDataAt(name_address)

#Try to define function name string.
if func_name is None:
    try:
        func_name = createAsciiString(name_address)
    except:
        print "ERROR: No name"
        continue
```

Binary: eCh0raix – x86

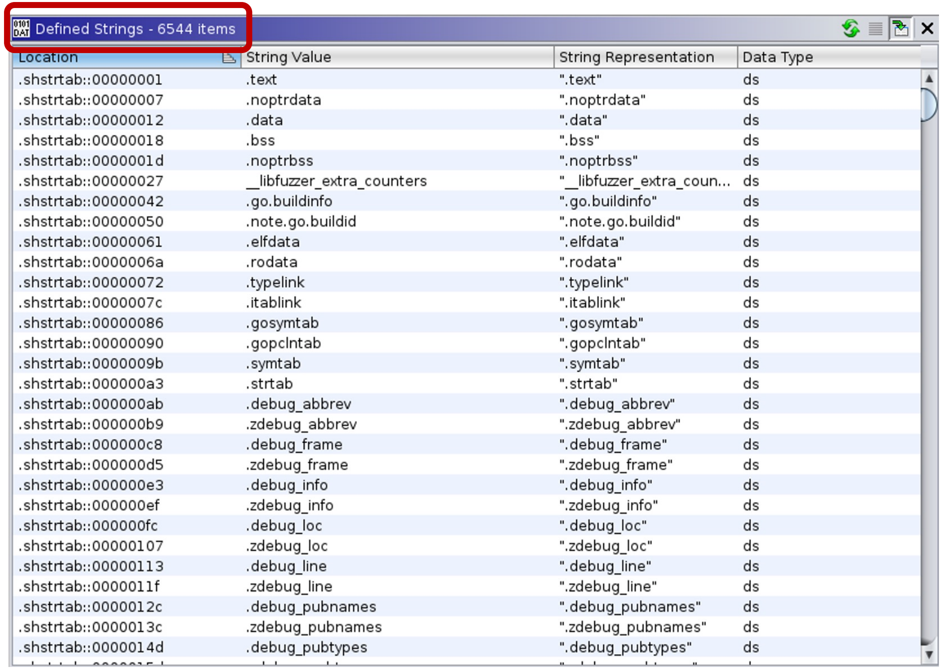
Hello World Strings in Ghidra

C vs Go



Defined Strings - 70 items

Location	String Value	String Representat...	Data Type
.strtab::000000db	__GNU_EH_FRAME_HDR	"__GNU_EH_FRAME_...	ds
.strtab::000000ee	_GLOBAL_OFFSET_TABLE_	"_GLOBAL_OFFSET_...	ds
.strtab::00000104	__libc_csu_fini	"__libc_csu_fini"	ds
.strtab::00000114	_ITM_deregisterTMCloneTable	"_ITM_deregisterTM...	ds
.strtab::00000130	puts@@GLIBC_2.2.5	"puts@@GLIBC_2.2...	ds
.strtab::00000142	_edata	"_edata"	ds
.strtab::00000149	__libc_start_main@@GLIBC_2.2.5	"__libc_start_main...	ds
.strtab::00000168	__data_start	"__data_start"	ds
.strtab::00000175	__gmon_start__	"__gmon_start__"	ds
.strtab::00000184	__dso_handle	"__dso_handle"	ds
.strtab::00000191	_IO_stdin_used	"_IO_stdin_used"	ds
.strtab::000001a0	__libc_csu_init	"__libc_csu_init"	ds
.strtab::000001b0	__bss_start	"__bss_start"	ds
.strtab::000001bc	main	"main"	ds
.strtab::000001c1	__TMC_END__	"__TMC_END__"	ds
.strtab::000001cd	_ITM_registerTMCloneTable	"_ITM_registerTMCl...	ds
.strtab::000001e7	__cxa_finalize@@GLIBC_2.2.5	"__cxa_finalize@@G...	ds
00100001	ELF	"ELF"	ds
00100318	/lib64/ld-linux-x86-64.so.2	"/lib64/ld-linux-x86-...	ds
00100471	libc.so.6	"libc.so.6"	ds
0010047b	puts	"puts"	ds
00100480	__cxa_finalize	"__cxa_finalize"	ds
0010048f	__libc_start_main	"__libc_start_main"	ds
001004a1	GLIBC_2.2.5	"GLIBC_2.2.5"	ds
001004ad	_ITM_deregisterTMCloneTable	"_ITM_deregisterTM...	ds
001004c9	__gmon_start__	"__gmon_start__"	ds
001004d8	_ITM_registerTMCloneTable	"_ITM_registerTMCl...	ds
00102004	Hello, World!	"Hello, World!"	ds
00102061	zR	"zR"	ds



Defined Strings - 6544 items

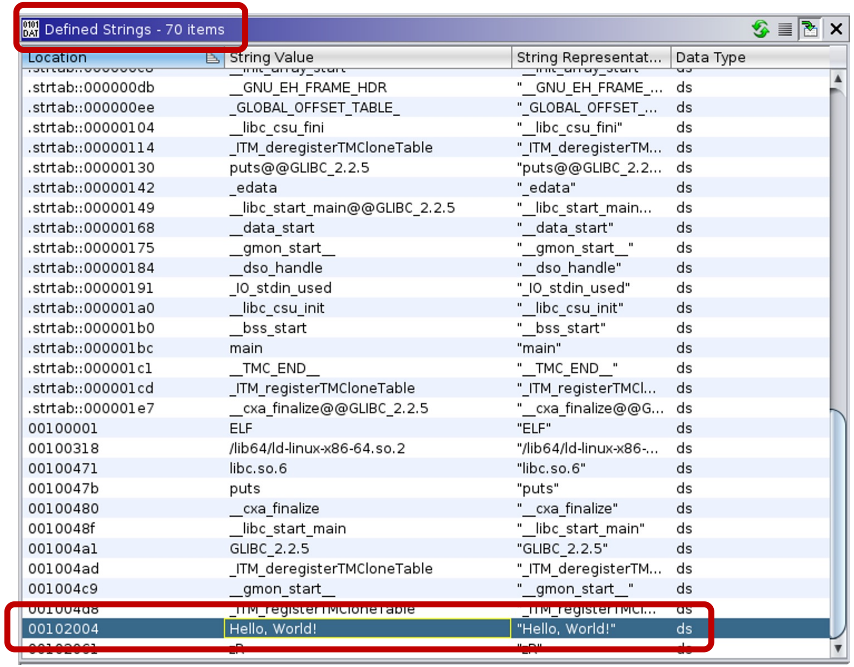
Location	String Value	String Representation	Data Type
.shstrtab::00000001	.text	".text"	ds
.shstrtab::00000007	.noptrdata	".noptrdata"	ds
.shstrtab::00000012	.data	".data"	ds
.shstrtab::00000018	.bss	".bss"	ds
.shstrtab::0000001d	.noptrbss	".noptrbss"	ds
.shstrtab::00000027	__libfuzzer_extra_counters	"__libfuzzer_extra_coun...	ds
.shstrtab::00000042	.go.buildinfo	".go.buildinfo"	ds
.shstrtab::00000050	.note.go.buildid	".note.go.buildid"	ds
.shstrtab::00000061	.elfdata	".elfdata"	ds
.shstrtab::0000006a	.rodata	".rodata"	ds
.shstrtab::00000072	.typelink	".typelink"	ds
.shstrtab::0000007c	.itablink	".itablink"	ds
.shstrtab::00000086	.gosymtab	".gosymtab"	ds
.shstrtab::00000090	.gopclntab	".gopclntab"	ds
.shstrtab::0000009b	.symtab	".symtab"	ds
.shstrtab::000000a3	.strtab	".strtab"	ds
.shstrtab::000000ab	.debug_abbrev	".debug_abbrev"	ds
.shstrtab::000000b9	.zdebug_abbrev	".zdebug_abbrev"	ds
.shstrtab::000000c8	.debug_frame	".debug_frame"	ds
.shstrtab::000000d5	.zdebug_frame	".zdebug_frame"	ds
.shstrtab::000000e3	.debug_info	".debug_info"	ds
.shstrtab::000000ef	.zdebug_info	".zdebug_info"	ds
.shstrtab::000000fc	.debug_loc	".debug_loc"	ds
.shstrtab::00000107	.zdebug_loc	".zdebug_loc"	ds
.shstrtab::00000113	.debug_line	".debug_line"	ds
.shstrtab::0000011f	.zdebug_line	".zdebug_line"	ds
.shstrtab::0000012c	.debug_pubnames	".debug_pubnames"	ds
.shstrtab::0000013c	.zdebug_pubnames	".zdebug_pubnames"	ds
.shstrtab::0000014d	.debug_pubtypes	".debug_pubtypes"	ds

70 defined strings vs 6544 defined strings

Binaries: world_c, world_go

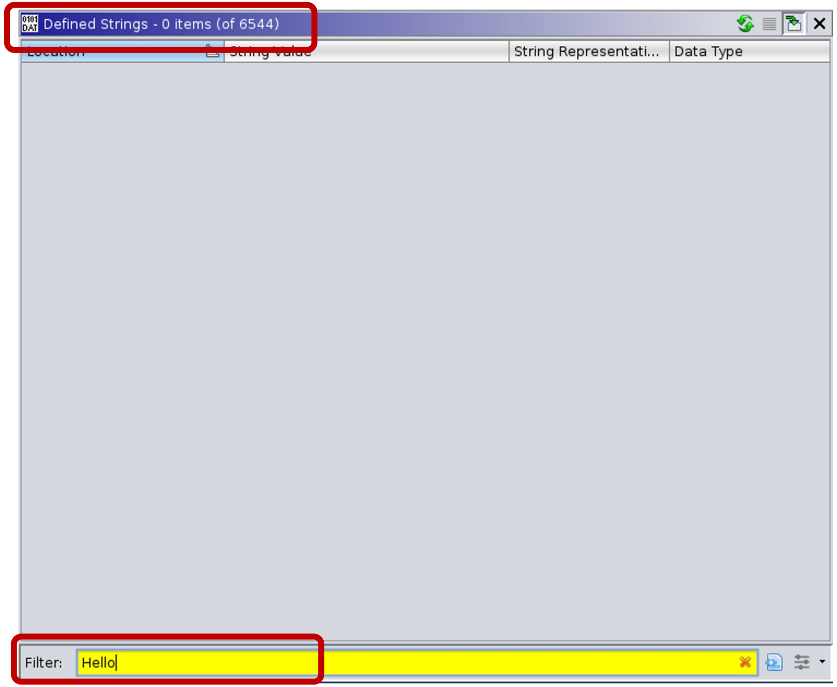
Hello World Strings in Ghidra

C vs Go



Defined Strings - 70 items

Location	String Value	String Representat...	Data Type
.strtab::000000c8	__init_array_start	"__init_array_start"	ds
.strtab::000000db	__GNU_EH_FRAME_HDR	"__GNU_EH_FRAME_...	ds
.strtab::000000ee	_GLOBAL_OFFSET_TABLE_	"_GLOBAL_OFFSET_...	ds
.strtab::00000104	__libc_csu_fini	"__libc_csu_fini"	ds
.strtab::00000114	_ITM_deregisterTMCloneTable	"_ITM_deregisterTM...	ds
.strtab::00000130	puts@@GLIBC_2.2.5	"puts@@GLIBC_2.2...	ds
.strtab::00000142	_edata	"_edata"	ds
.strtab::00000149	__libc_start_main@@GLIBC_2.2.5	"__libc_start_main...	ds
.strtab::00000168	__data_start	"__data_start"	ds
.strtab::00000175	__gmon_start__	"__gmon_start__"	ds
.strtab::00000184	__dso_handle	"__dso_handle"	ds
.strtab::00000191	_IO_stdin_used	"_IO_stdin_used"	ds
.strtab::000001a0	__libc_csu_init	"__libc_csu_init"	ds
.strtab::000001b0	__bss_start	"__bss_start"	ds
.strtab::000001bc	main	"main"	ds
.strtab::000001c1	__TMC_END__	"__TMC_END__"	ds
.strtab::000001cd	_ITM_registerTMCloneTable	"_ITM_registerTMCl...	ds
.strtab::000001e7	__cxa_finalize@@GLIBC_2.2.5	"__cxa_finalize@@G...	ds
00100001	ELF	"ELF"	ds
00100318	/lib64/ld-linux-x86-64.so.2	"/lib64/ld-linux-x86-...	ds
00100471	libc.so.6	"libc.so.6"	ds
0010047b	puts	"puts"	ds
00100480	__cxa_finalize	"__cxa_finalize"	ds
0010048f	__libc_start_main	"__libc_start_main"	ds
001004a1	GLIBC_2.2.5	"GLIBC_2.2.5"	ds
001004ad	_ITM_deregisterTMCloneTable	"_ITM_deregisterTM...	ds
001004c9	__gmon_start__	"__gmon_start__"	ds
001004d8	_ITM_registerTMCloneTable	"_ITM_registerTMCl...	ds
00102004	Hello, World!	"Hello, World!"	ds
00102061	zR	"zR"	ds



Defined Strings - 0 items (of 6544)

Location	String Value	String Representati...	Data Type

Filter: Hello

No “Hello” in Go

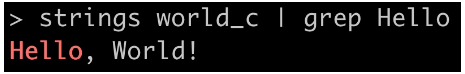
Binaries: world_c, world_go

Hello World Strings

C vs Go

C:

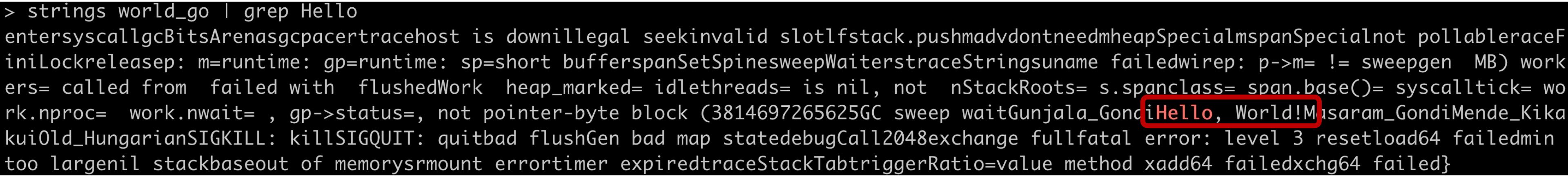
“Hello, World!” is easy to find



```
> strings world_c | grep Hello
Hello, World!
```

Go:

“Hello, World!” is part of a huge string



```
> strings world_go | grep Hello
entersyscallgcBitsArenasgcpacertracehost is downillegal seekinvalid slotlfstack.pushmadvdontneedmheapSpecialmspanSpecialnot pollableraceF
iniLockreleasep: m=runtime: gp=runtime: sp=short bufferspanSetSpinesweepWaiterstraceStringsuname failedwirep: p->m= != sweepgen  MB) work
ers= called from  failed with  flushedWork  heap_marked= idlethreads= is nil, not  nStackRoots= s.spanclass= span.base()= syscalltick= wo
rk.nproc=  work.nwait= , gp->status=, not pointer-byte block (3814697265625GC sweep waitGunjala_GondiHello, World!Masaram_GondiMende_Kika
kuiOld_HungarianSIGKILL: killSIGQUIT: quitbad flushGen bad map statedebugCall2048exchange fullfatal error: level 3 resetload64 failedmin
too largenil stackbaseout of memorysrmount errortimer expiredtraceStackTabtriggerRatio=value method xadd64 failedxchg64 failed}
```

Binaries: world_c, world_go_println

String Representation

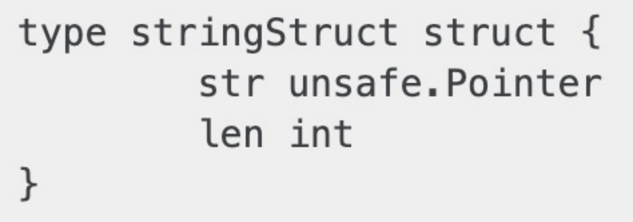
C vs Go

C

- sequence of characters terminated with a null character

Go

- sequence of bytes with a fixed length
- not null terminated
- str – sequence of bytes
- len – number of bytes
- https://golang.org/src/runtime/string.go
- Large string blobs from concatenated strings until null character
- Ghidra has a hard time defining strings in Go binaries



```
type stringStruct struct {
        str unsafe.Pointer
        len int
}
```

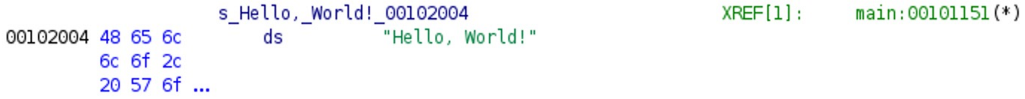
Idea: help Ghidra to find string structures

- Static vs dynamic allocation
- Per architecture (different instruction set)
- Multiple solution within one architecture
- Possible changes per Go version

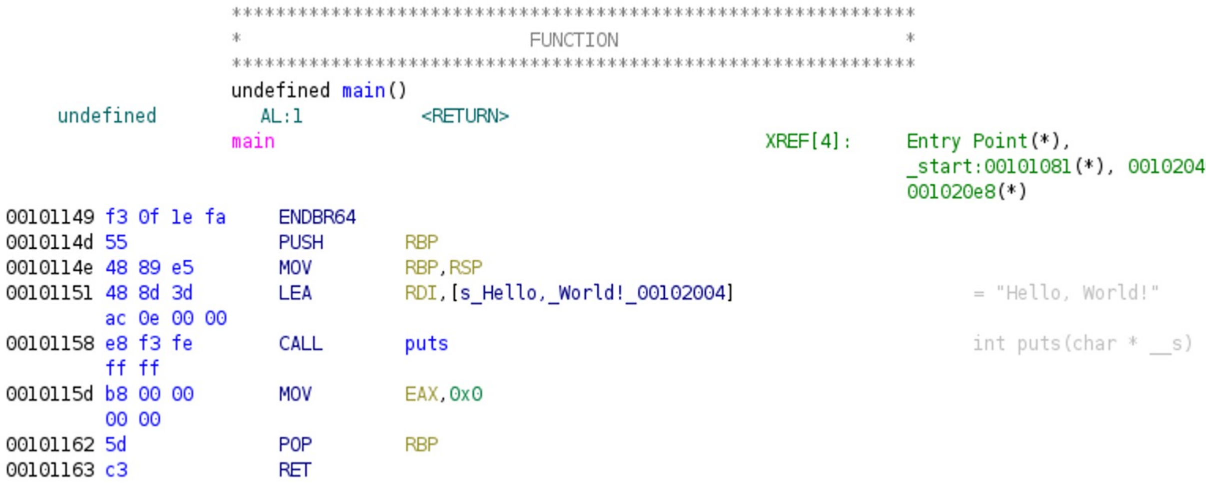
Dynamically allocated string structure

x86

- String structures can be allocated runtime
- Several different scenarios
- Let’s look at the Hello World examples again



```
                        s_Hello,_World!_00102004                    XREF[1]:     main:00101151(*)
00102004 48 65 6c           ds          "Hello, World!"
         6c 6f 2c
         20 57 6f ...
```

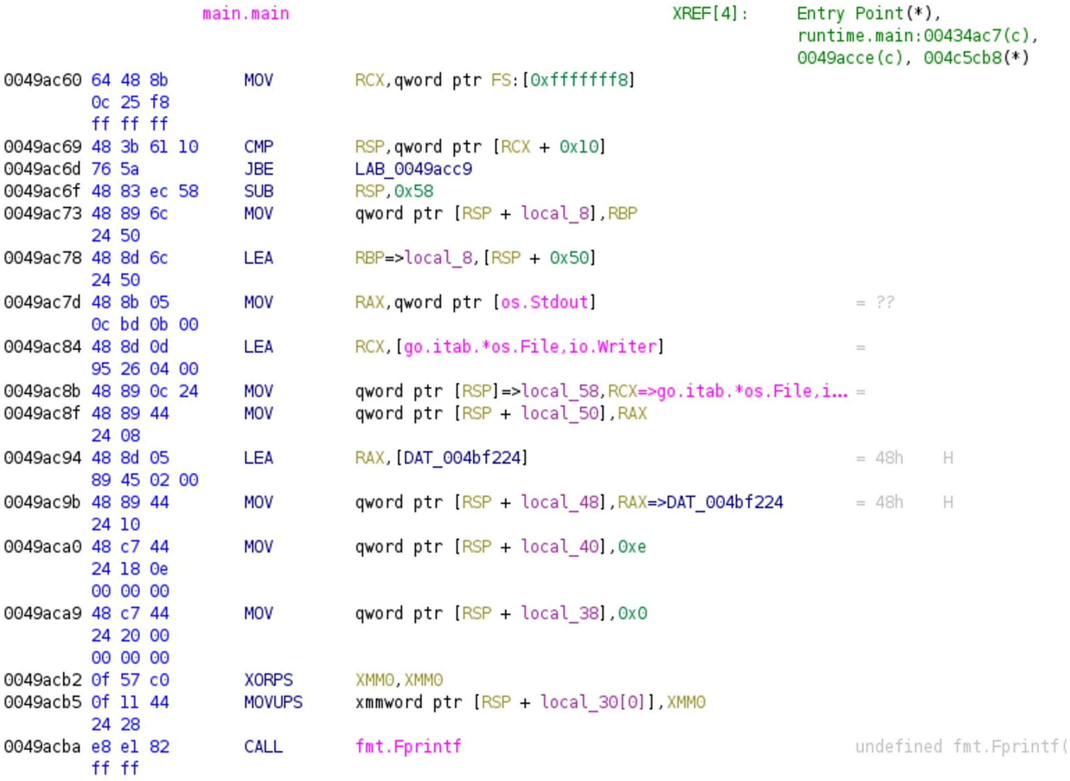


```
                   **************************************************************
                   *                          FUNCTION                          *
                   **************************************************************
                   undefined main()
     undefined        AL:1           <RETURN>
                   main                                      XREF[4]:     Entry Point(*),
                                                                          _start:00101081(*), 00102040,
                                                                          001020e8(*)
00101149 f3 0f 1e fa      ENDBR64
0010114d 55               PUSH       RBP
0010114e 48 89 e5         MOV        RBP,RSP
00101151 48 8d 3d         LEA        RDI,[s_Hello,_World!_00102004]                = "Hello, World!"
         ac 0e 00 00
00101158 e8 f3 fe         CALL       puts                                          int puts(char * __s)
         ff ff
0010115d b8 00 00         MOV        EAX,0x0
         00 00
00101162 5d               POP        RBP
00101163 c3               RET
```

Binary: world_c

Dynamically allocated string structure

x86

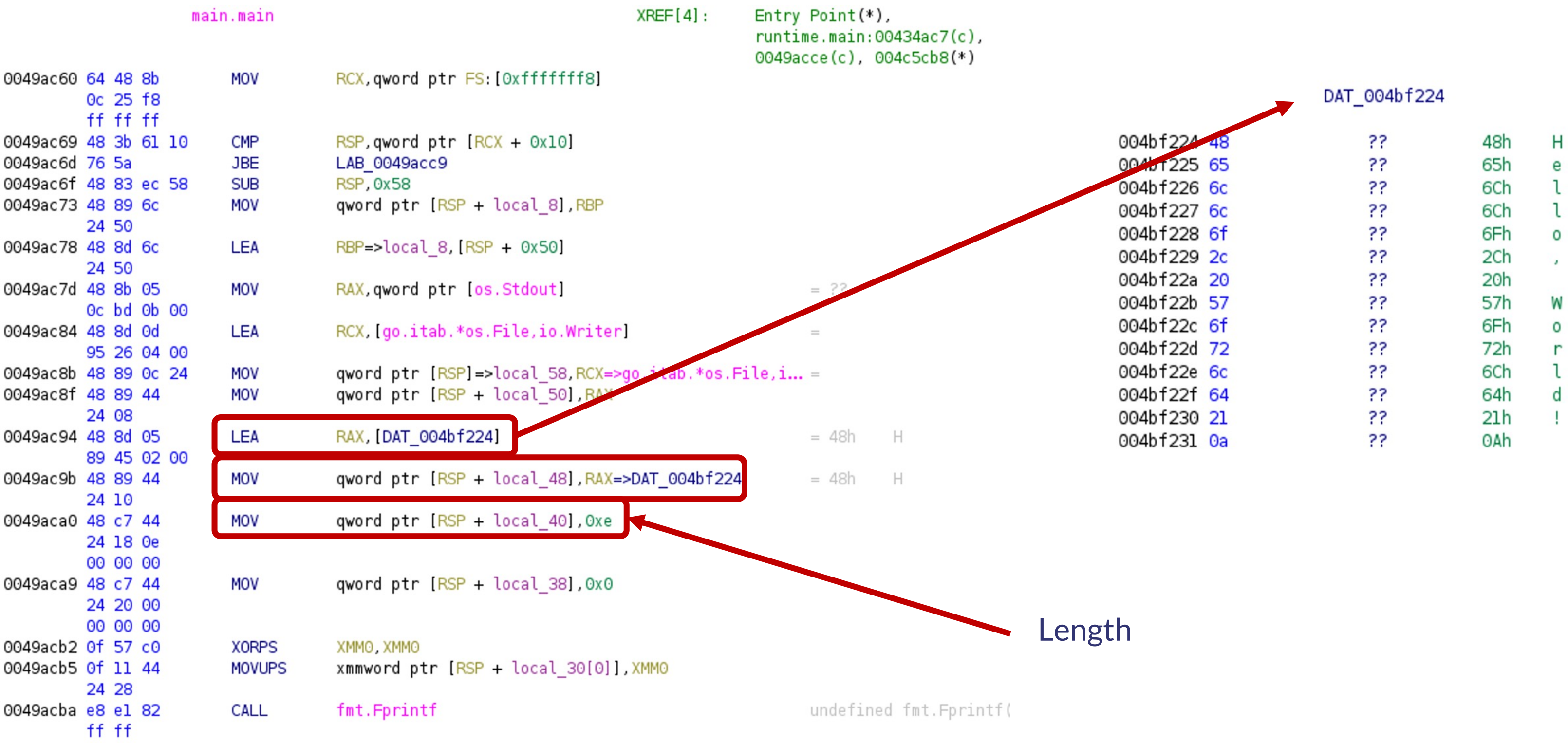


```
                    main.main                            XREF[4]:     Entry Point(*),
                                                                      runtime.main:00434ac7(c),
                                                                      0049acce(c), 004c5cb8(*)
0049ac60 64 48 8b       MOV       RCX,qword ptr FS:[0xfffffff8]
         0c 25 f8
         ff ff ff
0049ac69 48 3b 61 10    CMP       RSP,qword ptr [RCX + 0x10]
0049ac6d 76 5a          JBE       LAB_0049acc9
0049ac6f 48 83 ec 58    SUB       RSP,0x58
0049ac73 48 89 6c       MOV       qword ptr [RSP + local_8],RBP
         24 50
0049ac78 48 8d 6c       LEA       RBP=>local_8,[RSP + 0x50]
         24 50
0049ac7d 48 8b 05       MOV       RAX,qword ptr [os.Stdout]                    = ??
         0c bd 0b 00
0049ac84 48 8d 0d       LEA       RCX,[go.itab.*os.File,io.Writer]             =
         95 26 04 00
0049ac8b 48 89 0c 24    MOV       qword ptr [RSP]=>local_58,RCX=>go.itab.*os.File,i… =
0049ac8f 48 89 44       MOV       qword ptr [RSP + local_50],RAX
         24 08
0049ac94 48 8d 05       LEA       RAX,[DAT_004bf224]                           = 48h     H
         89 45 02 00
0049ac9b 48 89 44       MOV       qword ptr [RSP + local_48],RAX=>DAT_004bf224 = 48h     H
         24 10
0049aca0 48 c7 44       MOV       qword ptr [RSP + local_40],0xe
         24 18 0e
         00 00 00
0049aca9 48 c7 44       MOV       qword ptr [RSP + local_38],0x0
         24 20 00
         00 00 00
0049acb2 0f 57 c0       XORPS     XMM0,XMM0
0049acb5 0f 11 44       MOVUPS    xmmword ptr [RSP + local_30[0]],XMM0
         24 28
0049acba e8 e1 82       CALL      fmt.Fprintf                                  undefined fmt.Fprintf(
         ff ff
```

Binary: world_go

Dynamically allocated string structure

x86



```
                   main.main                                  XREF[4]:     Entry Point(*),
                                                                           runtime.main:00434ac7(c),
                                                                           0049acce(c), 004c5cb8(*)
0049ac60 64 48 8b      MOV       RCX,qword ptr FS:[0xfffffff8]
         0c 25 f8
         ff ff ff
0049ac69 48 3b 61 10   CMP       RSP,qword ptr [RCX + 0x10]
0049ac6d 76 5a         JBE       LAB_0049acc9
0049ac6f 48 83 ec 58   SUB       RSP,0x58
0049ac73 48 89 6c      MOV       qword ptr [RSP + local_8],RBP
         24 50
0049ac78 48 8d 6c      LEA       RBP=>local_8,[RSP + 0x50]
         24 50
0049ac7d 48 8b 05      MOV       RAX,qword ptr [os.Stdout]                       = ??
         0c bd 0b 00
0049ac84 48 8d 0d      LEA       RCX,[go.itab.*os.File,io.Writer]                =
         95 26 04 00
0049ac8b 48 89 0c 24   MOV       qword ptr [RSP]=>local_58,RCX=>go.itab.*os.File,i... =
0049ac8f 48 89 44      MOV       qword ptr [RSP + local_50],RAX
         24 08
0049ac94 48 8d 05      LEA       RAX,[DAT_004bf224]                              = 48h    H
         89 45 02 00
0049ac9b 48 89 44      MOV       qword ptr [RSP + local_48],RAX=>DAT_004bf224    = 48h    H
         24 10
0049aca0 48 c7 44      MOV       qword ptr [RSP + local_40],0xe
         24 18 0e
         00 00 00
0049aca9 48 c7 44      MOV       qword ptr [RSP + local_38],0x0
         24 20 00
         00 00 00
0049acb2 0f 57 c0      XORPS     XMM0,XMM0
0049acb5 0f 11 44      MOVUPS    xmmword ptr [RSP + local_30[0]],XMM0
         24 28
0049acba e8 e1 82      CALL      fmt.Fprintf                                     undefined fmt.Fprintf(
         ff ff
```

```
                       DAT_004bf224
004bf224 48        ??        48h    H
004bf225 65        ??        65h    e
004bf226 6c        ??        6Ch    l
004bf227 6c        ??        6Ch    l
004bf228 6f        ??        6Fh    o
004bf229 2c        ??        2Ch    ,
004bf22a 20        ??        20h
004bf22b 57        ??        57h    W
004bf22c 6f        ??        6Fh    o
004bf22d 72        ??        72h    r
004bf22e 6c        ??        6Ch    l
004bf22f 64        ??        64h    d
004bf230 21        ??        21h    !
004bf231 0a        ??        0Ah
```

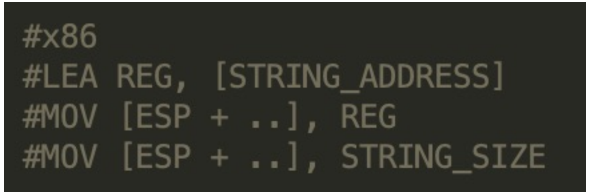
Length

Binary: world_go

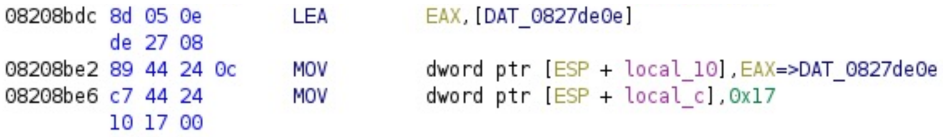
Dynamically allocated string structure

x86

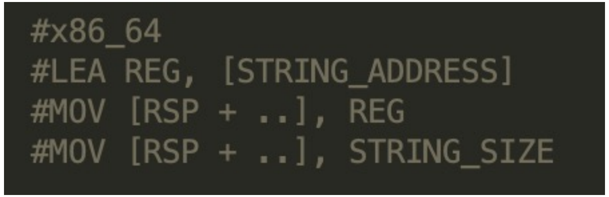
- Search for these instructions and define strings



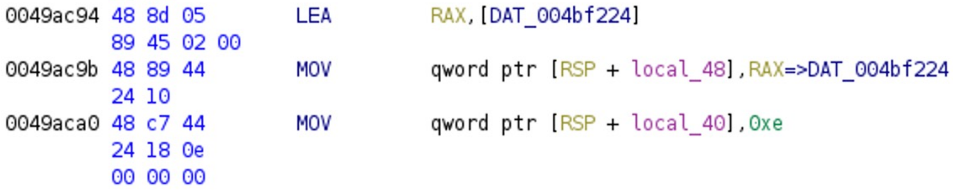
```
#x86
#LEA REG, [STRING_ADDRESS]
#MOV [ESP + ..], REG
#MOV [ESP + ..], STRING_SIZE
```



```
08208bdc 8d 05 0e       LEA      EAX,[DAT_0827de0e]
         de 27 08
08208be2 89 44 24 0c    MOV      dword ptr [ESP + local_10],EAX=>DAT_0827de0e
08208be6 c7 44 24       MOV      dword ptr [ESP + local_c],0x17
         10 17 00
```



```
#x86_64
#LEA REG, [STRING_ADDRESS]
#MOV [RSP + ..], REG
#MOV [RSP + ..], STRING_SIZE
```



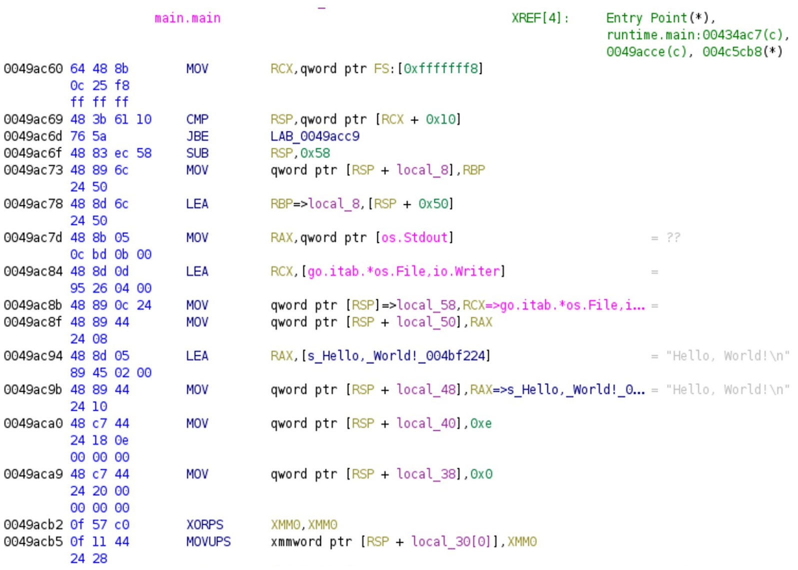
```
0049ac94 48 8d 05       LEA      RAX,[DAT_004bf224]
         89 45 02 00
0049ac9b 48 89 44       MOV      qword ptr [RSP + local_48],RAX=>DAT_004bf224
         24 10
0049aca0 48 c7 44       MOV      qword ptr [RSP + local_40],0xe
         24 18 0e
         00 00 00
```

Binary: eCh0raix – x86, world_go

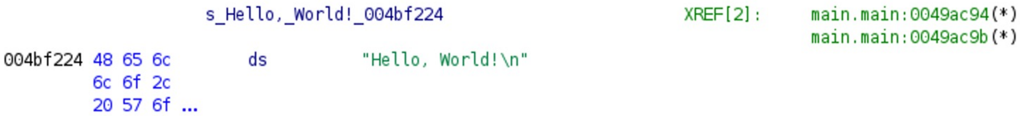
Dynamically allocated string structure

x86

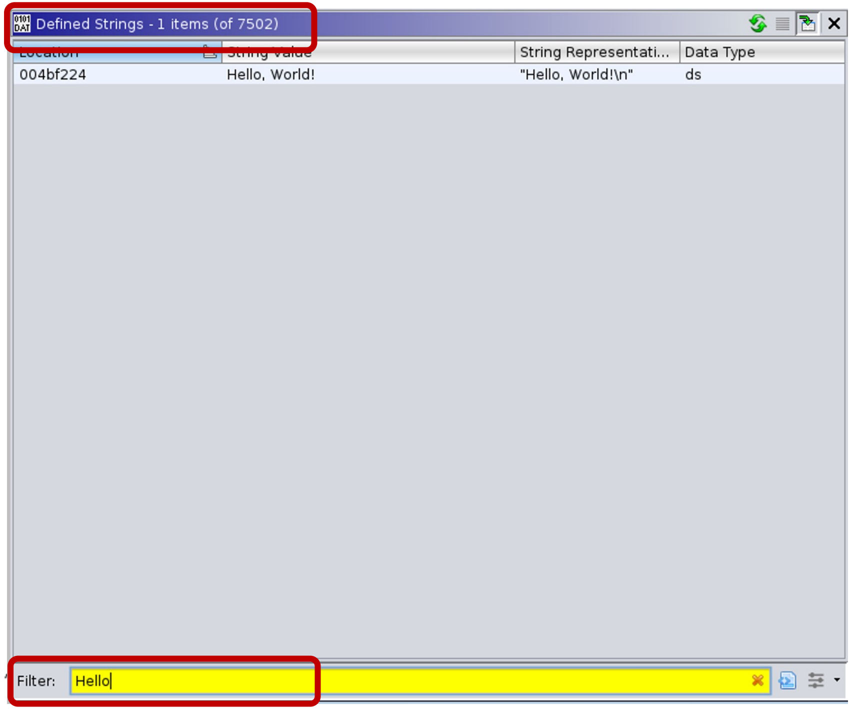
- Results after executing the script



```
                     main.main                          XREF[4]:    Entry Point(*),
                                                                    runtime.main:00434ac7(c),
                                                                    0049acce(c), 004c5cb8(*)
0049ac60 64 48 8b     MOV      RCX,qword ptr FS:[0xfffffff8]
         0c 25 f8
         ff ff ff
0049ac69 48 3b 61 10  CMP      RSP,qword ptr [RCX + 0x10]
0049ac6d 76 5a        JBE      LAB_0049acc9
0049ac6f 48 83 ec 58  SUB      RSP,0x58
0049ac73 48 89 6c     MOV      qword ptr [RSP + local_8],RBP
         24 50
0049ac78 48 8d 6c     LEA      RBP=>local_8,[RSP + 0x50]
         24 50
0049ac7d 48 8b 05     MOV      RAX,qword ptr [os.Stdout]                        = ??
         0c bd 0b 00
0049ac84 48 8d 0d     LEA      RCX,[go.itab.*os.File,io.Writer]                 =
         95 26 04 00
0049ac8b 48 89 0c 24  MOV      qword ptr [RSP]=>local_58,RCX=>go.itab.*os.File,i... =
0049ac8f 48 89 44     MOV      qword ptr [RSP + local_50],RAX
         24 08
0049ac94 48 8d 05     LEA      RAX,[s_Hello,_World!_004bf224]                   = "Hello, World!\n"
         89 45 02 00
0049ac9b 48 89 44     MOV      qword ptr [RSP + local_48],RAX=>s_Hello,_World!_0... = "Hello, World!\n"
         24 10
0049aca0 48 c7 44     MOV      qword ptr [RSP + local_40],0xe
         24 18 0e
         00 00 00
0049aca9 48 c7 44     MOV      qword ptr [RSP + local_38],0x0
         24 20 00
         00 00 00
0049acb2 0f 57 c0     XORPS    XMM0,XMM0
0049acb5 0f 11 44     MOVUPS   xmmword ptr [RSP + local_30[0]],XMM0
         24 28
```



```
               s_Hello,_World!_004bf224               XREF[2]:    main.main:0049ac94(*),
                                                                  main.main:0049ac9b(*)
004bf224 48 65 6c       ds          "Hello, World!\n"
         6c 6f 2c
         20 57 6f ...
```



Defined Strings - 1 items (of 7502)

Location	String Value	String Representati...	Data Type
004bf224	Hello, World!	"Hello, World!\n"	ds

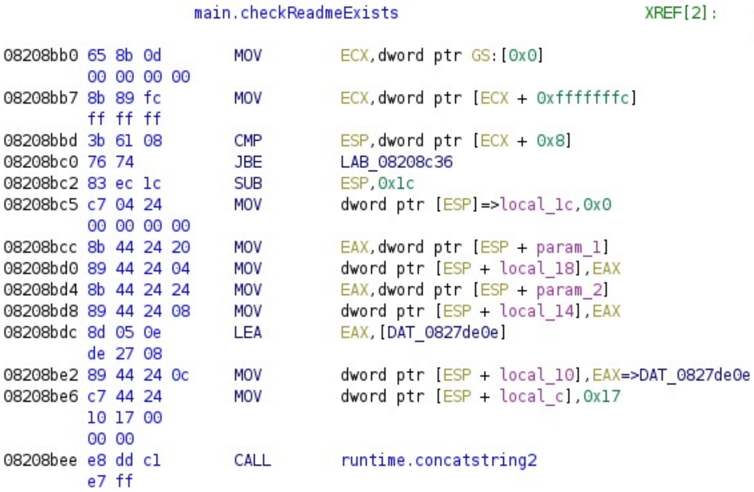
Filter: Hello

Binary: world_go

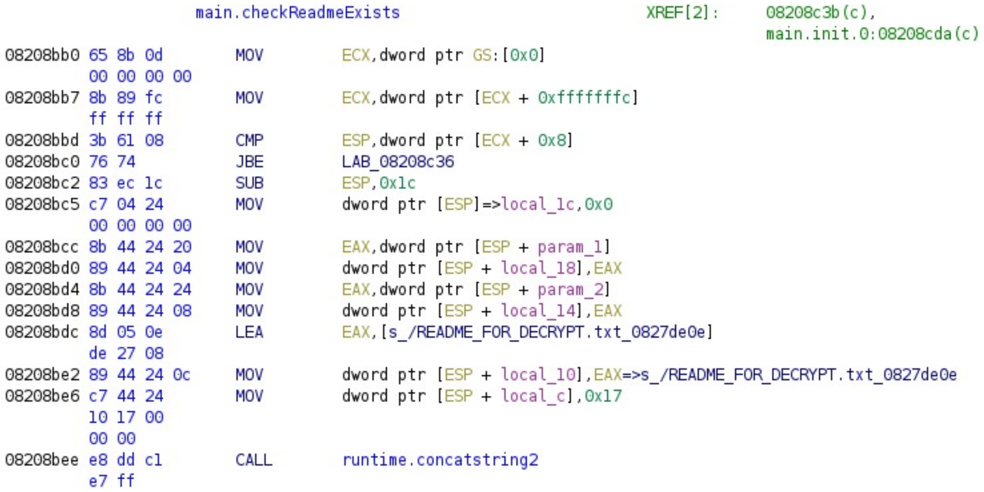
Dynamically allocated string structure

x86

- After executing our script the number of defined strings grew from 9719 to 11213



```
                      main.checkReadmeExists                          XREF[2]:     08208c3b(c),
                                                                                   main.init.0:08208cda(c)
08208bb0 65 8b 0d        MOV        ECX,dword ptr GS:[0x0]
         00 00 00 00
08208bb7 8b 89 fc        MOV        ECX,dword ptr [ECX + 0xfffffffc]
         ff ff ff
08208bbd 3b 61 08        CMP        ESP,dword ptr [ECX + 0x8]
08208bc0 76 74           JBE        LAB_08208c36
08208bc2 83 ec 1c        SUB        ESP,0x1c
08208bc5 c7 04 24        MOV        dword ptr [ESP]=>local_1c,0x0
         00 00 00 00
08208bcc 8b 44 24 20     MOV        EAX,dword ptr [ESP + param_1]
08208bd0 89 44 24 04     MOV        dword ptr [ESP + local_18],EAX
08208bd4 8b 44 24 24     MOV        EAX,dword ptr [ESP + param_2]
08208bd8 89 44 24 08     MOV        dword ptr [ESP + local_14],EAX
08208bdc 8d 05 0e        LEA        EAX,[DAT_0827de0e]
         de 27 08
08208be2 89 44 24 0c     MOV        dword ptr [ESP + local_10],EAX=>DAT_0827de0e
08208be6 c7 44 24        MOV        dword ptr [ESP + local_c],0x17
         10 17 00
         00 00
08208bee e8 dd c1        CALL       runtime.concatstring2
         e7 ff
```

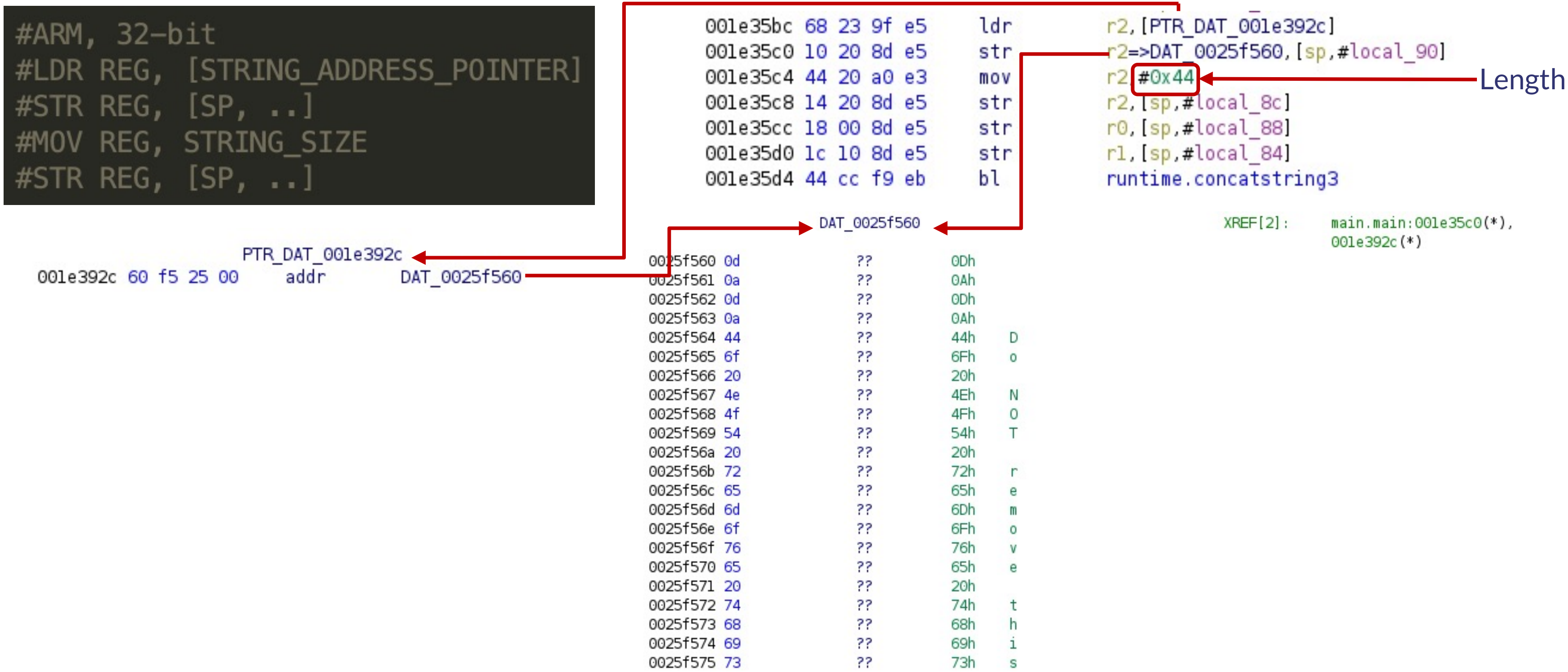


```
                      main.checkReadmeExists                          XREF[2]:     08208c3b(c),
                                                                                   main.init.0:08208cda(c)
08208bb0 65 8b 0d        MOV        ECX,dword ptr GS:[0x0]
         00 00 00 00
08208bb7 8b 89 fc        MOV        ECX,dword ptr [ECX + 0xfffffffc]
         ff ff ff
08208bbd 3b 61 08        CMP        ESP,dword ptr [ECX + 0x8]
08208bc0 76 74           JBE        LAB_08208c36
08208bc2 83 ec 1c        SUB        ESP,0x1c
08208bc5 c7 04 24        MOV        dword ptr [ESP]=>local_1c,0x0
         00 00 00 00
08208bcc 8b 44 24 20     MOV        EAX,dword ptr [ESP + param_1]
08208bd0 89 44 24 04     MOV        dword ptr [ESP + local_18],EAX
08208bd4 8b 44 24 24     MOV        EAX,dword ptr [ESP + param_2]
08208bd8 89 44 24 08     MOV        dword ptr [ESP + local_14],EAX
08208bdc 8d 05 0e        LEA        EAX,[s_/README_FOR_DECRYPT.txt_0827de0e]
         de 27 08
08208be2 89 44 24 0c     MOV        dword ptr [ESP + local_10],EAX=>s_/README_FOR_DECRYPT.txt_0827de0e
08208be6 c7 44 24        MOV        dword ptr [ESP + local_c],0x17
         10 17 00
         00 00
08208bee e8 dd c1        CALL       runtime.concatstring2
         e7 ff
```

Binary: eCh0raix – x86

Dynamically allocated string structure

ARM – before executing the script



```
#ARM, 32-bit
#LDR REG, [STRING_ADDRESS_POINTER]
#STR REG, [SP, ..]
#MOV REG, STRING_SIZE
#STR REG, [SP, ..]
```

```
001e35bc 68 23 9f e5     ldr        r2,[PTR_DAT_001e392c]
001e35c0 10 20 8d e5     str        r2=>DAT_0025f560,[sp,#local_90]
001e35c4 44 20 a0 e3     mov        r2,#0x44
001e35c8 14 20 8d e5     str        r2,[sp,#local_8c]
001e35cc 18 00 8d e5     str        r0,[sp,#local_88]
001e35d0 1c 10 8d e5     str        r1,[sp,#local_84]
001e35d4 44 cc f9 eb     bl         runtime.concatstring3
```

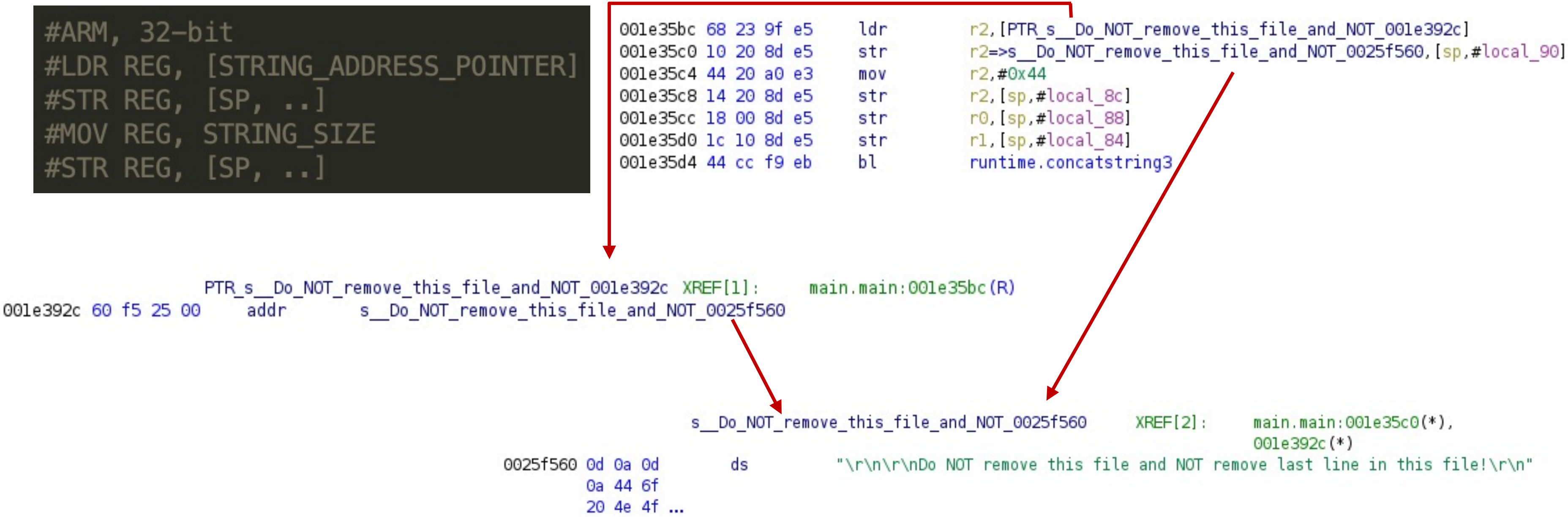
```
              PTR_DAT_001e392c
001e392c 60 f5 25 00     addr        DAT_0025f560
```

```
                         DAT_0025f560                    XREF[2]:     main.main:001e35c0(*),
                                                                      001e392c(*)
0025f560 0d          ??          0Dh
0025f561 0a          ??          0Ah
0025f562 0d          ??          0Dh
0025f563 0a          ??          0Ah
0025f564 44          ??          44h    D
0025f565 6f          ??          6Fh    o
0025f566 20          ??          20h
0025f567 4e          ??          4Eh    N
0025f568 4f          ??          4Fh    O
0025f569 54          ??          54h    T
0025f56a 20          ??          20h
0025f56b 72          ??          72h    r
0025f56c 65          ??          65h    e
0025f56d 6d          ??          6Dh    m
0025f56e 6f          ??          6Fh    o
0025f56f 76          ??          76h    v
0025f570 65          ??          65h    e
0025f571 20          ??          20h
0025f572 74          ??          74h    t
0025f573 68          ??          68h    h
0025f574 69          ??          69h    i
0025f575 73          ??          73h    s
```

Binary: eCh0raix – ARM

Dynamically allocated string structure

ARM – after executing the script



```
#ARM, 32-bit
#LDR REG, [STRING_ADDRESS_POINTER]
#STR REG, [SP, ..]
#MOV REG, STRING_SIZE
#STR REG, [SP, ..]
```

```
001e35bc 68 23 9f e5     ldr        r2,[PTR_s__Do_NOT_remove_this_file_and_NOT_001e392c]
001e35c0 10 20 8d e5     str        r2=>s__Do_NOT_remove_this_file_and_NOT_0025f560,[sp,#local_90]
001e35c4 44 20 a0 e3     mov        r2,#0x44
001e35c8 14 20 8d e5     str        r2,[sp,#local_8c]
001e35cc 18 00 8d e5     str        r0,[sp,#local_88]
001e35d0 1c 10 8d e5     str        r1,[sp,#local_84]
001e35d4 44 cc f9 eb     bl         runtime.concatstring3
```

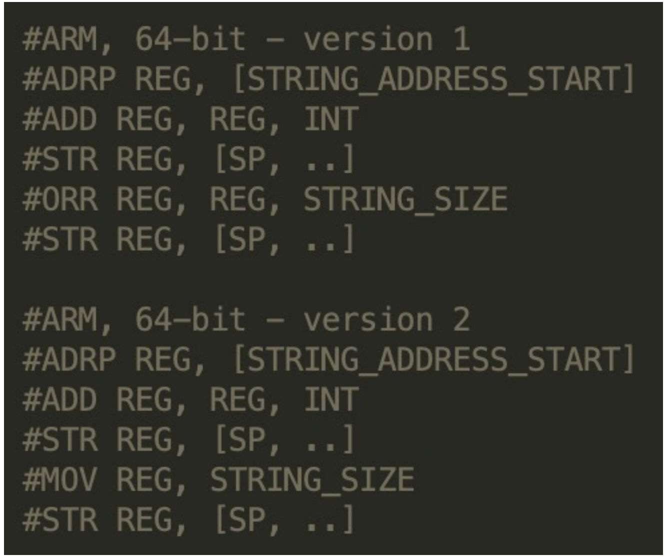
```
                PTR_s__Do_NOT_remove_this_file_and_NOT_001e392c  XREF[1]:     main.main:001e35bc(R)
001e392c 60 f5 25 00     addr       s__Do_NOT_remove_this_file_and_NOT_0025f560
```

```
                    s__Do_NOT_remove_this_file_and_NOT_0025f560     XREF[2]:     main.main:001e35c0(*),
                                                                                 001e392c(*)
0025f560 0d 0a 0d        ds         "\r\n\r\nDo NOT remove this file and NOT remove last line in this file!\r\n"
         0a 44 6f
         20 4e 4f ...
```

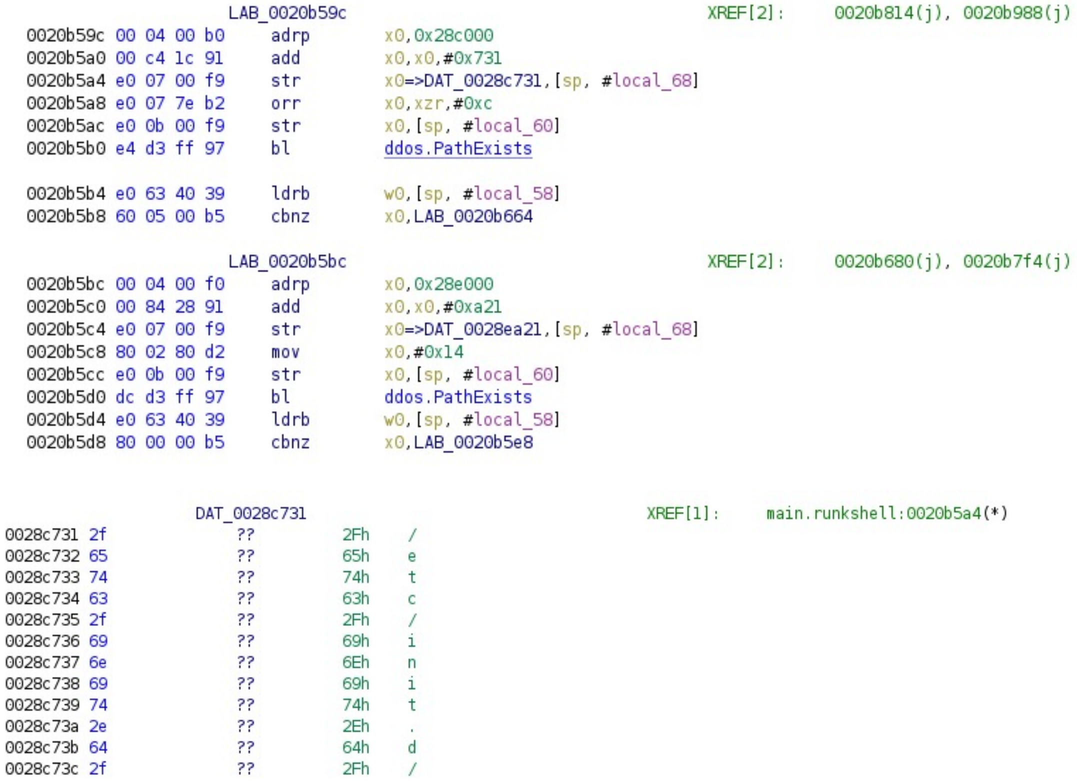
Binary: eCh0raix – ARM

Dynamically allocated string structure

ARM – before executing the script



```
#ARM, 64-bit - version 1
#ADRP REG, [STRING_ADDRESS_START]
#ADD REG, REG, INT
#STR REG, [SP, ..]
#ORR REG, REG, STRING_SIZE
#STR REG, [SP, ..]

#ARM, 64-bit - version 2
#ADRP REG, [STRING_ADDRESS_START]
#ADD REG, REG, INT
#STR REG, [SP, ..]
#MOV REG, STRING_SIZE
#STR REG, [SP, ..]
```

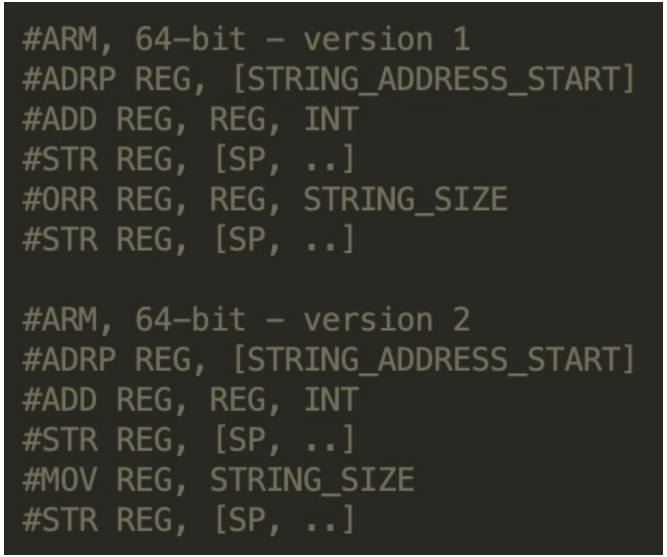


```
                        LAB_0020b59c                                     XREF[2]:     0020b814(j), 0020b988(j)
0020b59c 00 04 00 b0     adrp       x0,0x28c000
0020b5a0 00 c4 1c 91     add        x0,x0,#0x731
0020b5a4 e0 07 00 f9     str        x0=>DAT_0028c731,[sp, #local_68]
0020b5a8 e0 07 7e b2     orr        x0,xzr,#0xc
0020b5ac e0 0b 00 f9     str        x0,[sp, #local_60]
0020b5b0 e4 d3 ff 97     bl         ddos.PathExists

0020b5b4 e0 63 40 39     ldrb       w0,[sp, #local_58]
0020b5b8 60 05 00 b5     cbnz       x0,LAB_0020b664

                        LAB_0020b5bc                                     XREF[2]:     0020b680(j), 0020b7f4(j)
0020b5bc 00 04 00 f0     adrp       x0,0x28e000
0020b5c0 00 84 28 91     add        x0,x0,#0xa21
0020b5c4 e0 07 00 f9     str        x0=>DAT_0028ea21,[sp, #local_68]
0020b5c8 80 02 80 d2     mov        x0,#0x14
0020b5cc e0 0b 00 f9     str        x0,[sp, #local_60]
0020b5d0 dc d3 ff 97     bl         ddos.PathExists
0020b5d4 e0 63 40 39     ldrb       w0,[sp, #local_58]
0020b5d8 80 00 00 b5     cbnz       x0,LAB_0020b5e8


                      DAT_0028c731                                     XREF[1]:     main.runkshell:0020b5a4(*)
0028c731 2f           ??         2Fh    /
0028c732 65           ??         65h    e
0028c733 74           ??         74h    t
0028c734 63           ??         63h    c
0028c735 2f           ??         2Fh    /
0028c736 69           ??         69h    i
0028c737 6e           ??         6Eh    n
0028c738 69           ??         69h    i
0028c739 74           ??         74h    t
0028c73a 2e           ??         2Eh    .
0028c73b 64           ??         64h    d
0028c73c 2f           ??         2Fh    /
```

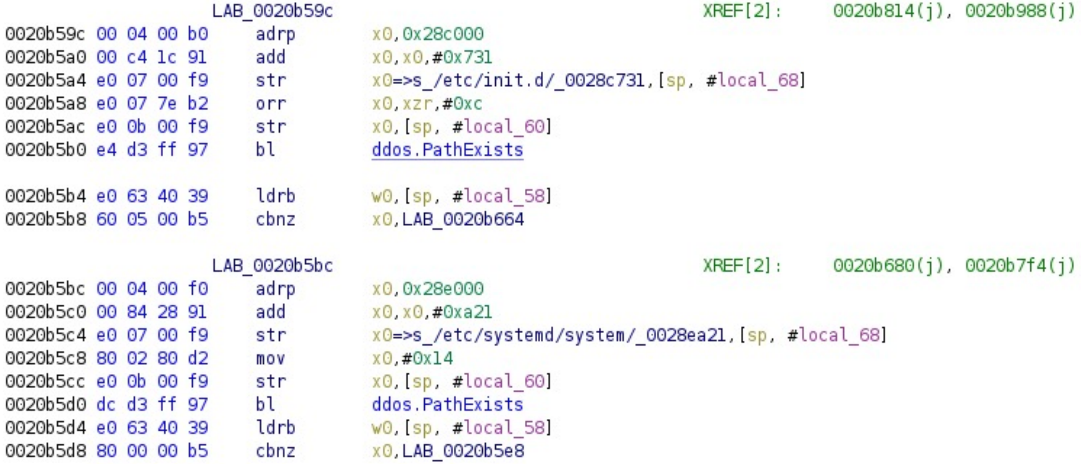
Binary: Kaiji – ARM

Dynamically allocated string structure

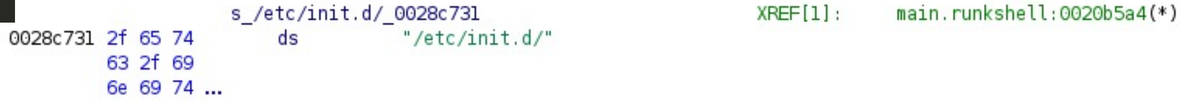
ARM – after executing the script



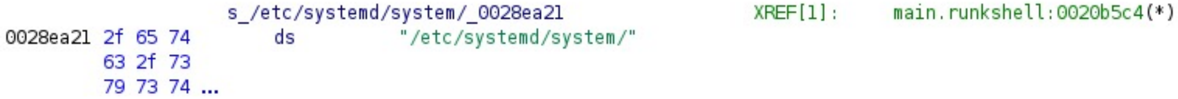
```
#ARM, 64-bit - version 1
#ADRP REG, [STRING_ADDRESS_START]
#ADD REG, REG, INT
#STR REG, [SP, ..]
#ORR REG, REG, STRING_SIZE
#STR REG, [SP, ..]

#ARM, 64-bit - version 2
#ADRP REG, [STRING_ADDRESS_START]
#ADD REG, REG, INT
#STR REG, [SP, ..]
#MOV REG, STRING_SIZE
#STR REG, [SP, ..]
```



```
                         LAB_0020b59c                                  XREF[2]:     0020b814(j), 0020b988(j)
0020b59c 00 04 00 b0     adrp       x0,0x28c000
0020b5a0 00 c4 1c 91     add        x0,x0,#0x731
0020b5a4 e0 07 00 f9     str        x0=>s_/etc/init.d/_0028c731,[sp, #local_68]
0020b5a8 e0 07 7e b2     orr        x0,xzr,#0xc
0020b5ac e0 0b 00 f9     str        x0,[sp, #local_60]
0020b5b0 e4 d3 ff 97     bl         ddos.PathExists

0020b5b4 e0 63 40 39     ldrb       w0,[sp, #local_58]
0020b5b8 60 05 00 b5     cbnz       x0,LAB_0020b664

                         LAB_0020b5bc                                  XREF[2]:     0020b680(j), 0020b7f4(j)
0020b5bc 00 04 00 f0     adrp       x0,0x28e000
0020b5c0 00 84 28 91     add        x0,x0,#0xa21
0020b5c4 e0 07 00 f9     str        x0=>s_/etc/systemd/system/_0028ea21,[sp, #local_68]
0020b5c8 80 02 80 d2     mov        x0,#0x14
0020b5cc e0 0b 00 f9     str        x0,[sp, #local_60]
0020b5d0 dc d3 ff 97     bl         ddos.PathExists
0020b5d4 e0 63 40 39     ldrb       w0,[sp, #local_58]
0020b5d8 80 00 00 b5     cbnz       x0,LAB_0020b5e8
```



```
                         s_/etc/init.d/_0028c731                          XREF[1]:     main.runkshell:0020b5a4(*)
0028c731 2f 65 74        ds         "/etc/init.d/"
         63 2f 69
         6e 69 74 ...
```



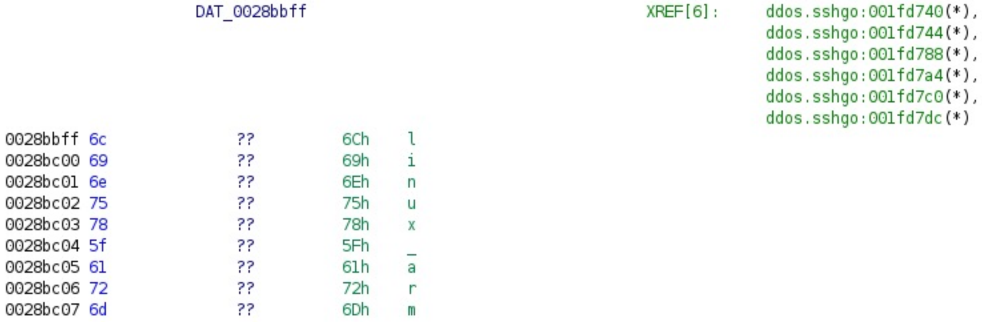
```
                         s_/etc/systemd/system/_0028ea21                  XREF[1]:     main.runkshell:0020b5c4(*)
0028ea21 2f 65 74        ds         "/etc/systemd/system/"
         63 2f 73
         79 73 74 ...
```

Binary: Kaiji – ARM

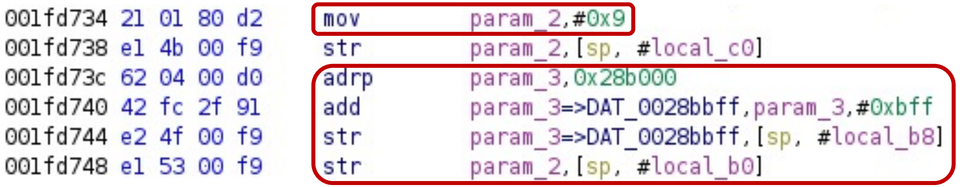
Dynamically allocated string structure

Challenges

- Different instruction sets
- Can be implemented in different ways within the same architecture
- Easy to break intentionally



```
                    DAT_0028bbff                           XREF[6]:     ddos.sshgo:001fd740(*),
                                                                        ddos.sshgo:001fd744(*),
                                                                        ddos.sshgo:001fd788(*),
                                                                        ddos.sshgo:001fd7a4(*),
                                                                        ddos.sshgo:001fd7c0(*),
                                                                        ddos.sshgo:001fd7dc(*)
0028bbff 6c            ??         6Ch    l
0028bc00 69            ??         69h    i
0028bc01 6e            ??         6Eh    n
0028bc02 75            ??         75h    u
0028bc03 78            ??         78h    x
0028bc04 5f            ??         5Fh    _
0028bc05 61            ??         61h    a
0028bc06 72            ??         72h    r
0028bc07 6d            ??         6Dh    m
```



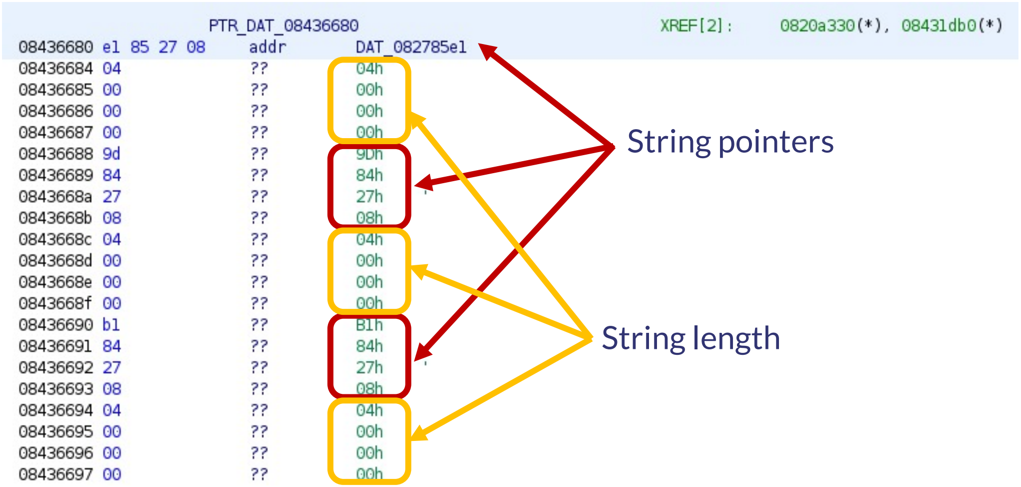
```
001fd734 21 01 80 d2    mov        param_2,#0x9
001fd738 e1 4b 00 f9    str        param_2,[sp, #local_c0]
001fd73c 62 04 00 d0    adrp       param_3,0x28b000
001fd740 42 fc 2f 91    add        param_3=>DAT_0028bbff,param_3,#0xbff
001fd744 e2 4f 00 f9    str        param_3=>DAT_0028bbff,[sp, #local_b8]
001fd748 e1 53 00 f9    str        param_2,[sp, #local_b0]
```

Binary: Kaiji – ARM

Statically allocated string structure

Idea

- Look for pointer to string followed by possible length value
- To eliminate FPs limit string length and search for printable characters only
- Check only in data sections
- Not architecture specific

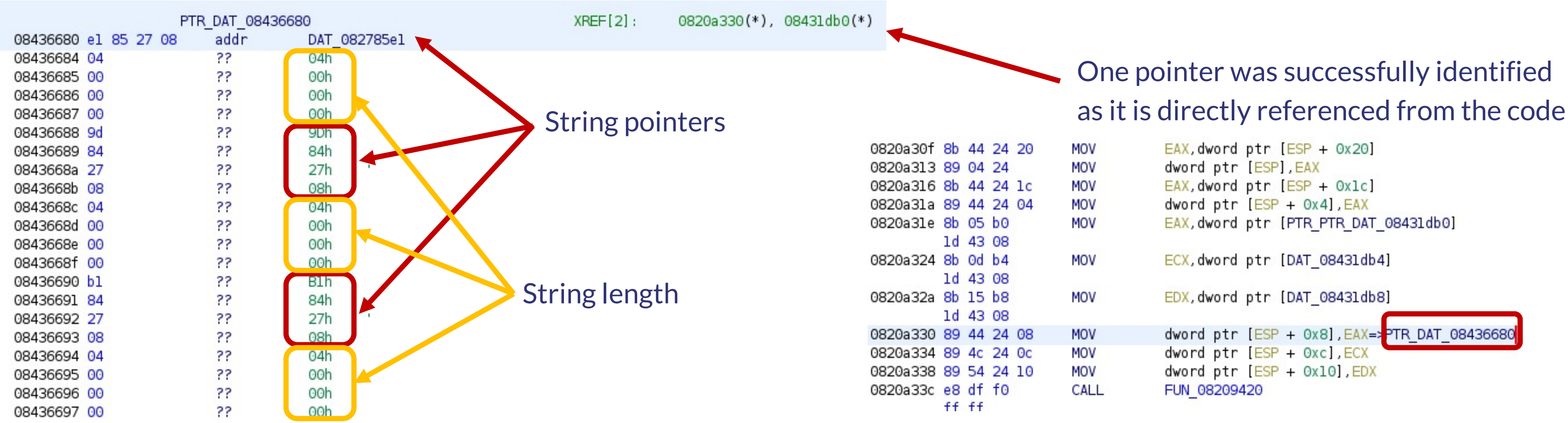


```
                      PTR_DAT_08436680                              XREF[2]:     0820a330(*), 08431db0(*)
08436680 e1 85 27 08      addr        DAT_082785e1
08436684 04               ??          04h
08436685 00               ??          00h
08436686 00               ??          00h
08436687 00               ??          00h
08436688 9d               ??          9Dh
08436689 84               ??          84h
0843668a 27               ??          27h
0843668b 08               ??          08h
0843668c 04               ??          04h
0843668d 00               ??          00h
0843668e 00               ??          00h
0843668f 00               ??          00h
08436690 b1               ??          B1h
08436691 84               ??          84h
08436692 27               ??          27h
08436693 08               ??          08h
08436694 04               ??          04h
08436695 00               ??          00h
08436696 00               ??          00h
08436697 00               ??          00h
```

Binary: eCh0raix – x86

Statically allocated string structure

Example – before executing the script



```
                    PTR_DAT_08436680                         XREF[2]:     0820a330(*), 08431db0(*)
08436680 e1 85 27 08     addr       DAT_082785e1
08436684 04              ??         04h
08436685 00              ??         00h
08436686 00              ??         00h
08436687 00              ??         00h
08436688 9d              ??         9Dh
08436689 84              ??         84h
0843668a 27              ??         27h
0843668b 08              ??         08h
0843668c 04              ??         04h
0843668d 00              ??         00h
0843668e 00              ??         00h
0843668f 00              ??         00h
08436690 b1              ??         B1h
08436691 84              ??         84h
08436692 27              ??         27h
08436693 08              ??         08h
08436694 04              ??         04h
08436695 00              ??         00h
08436696 00              ??         00h
08436697 00              ??         00h
```

String pointers

String length

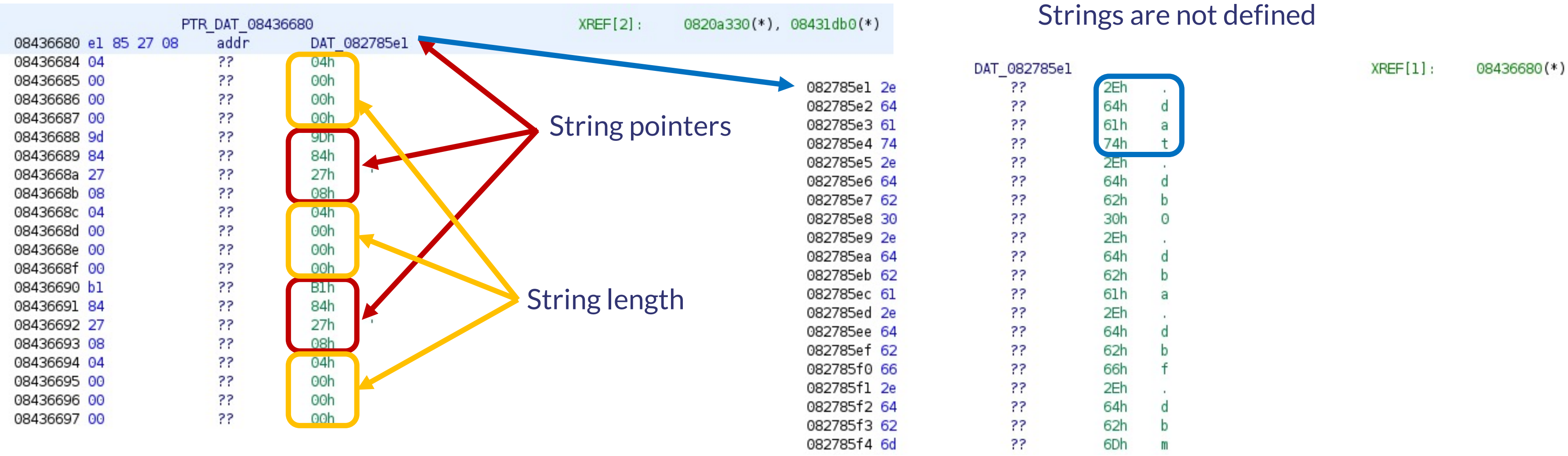
One pointer was successfully identified as it is directly referenced from the code

```
0820a30f 8b 44 24 20     MOV        EAX,dword ptr [ESP + 0x20]
0820a313 89 04 24        MOV        dword ptr [ESP],EAX
0820a316 8b 44 24 1c     MOV        EAX,dword ptr [ESP + 0x1c]
0820a31a 89 44 24 04     MOV        dword ptr [ESP + 0x4],EAX
0820a31e 8b 05 b0        MOV        EAX,dword ptr [PTR_PTR_DAT_08431db0]
         1d 43 08
0820a324 8b 0d b4        MOV        ECX,dword ptr [DAT_08431db4]
         1d 43 08
0820a32a 8b 15 b8        MOV        EDX,dword ptr [DAT_08431db8]
         1d 43 08
0820a330 89 44 24 08     MOV        dword ptr [ESP + 0x8],EAX=>PTR_DAT_08436680
0820a334 89 4c 24 0c     MOV        dword ptr [ESP + 0xc],ECX
0820a338 89 54 24 10     MOV        dword ptr [ESP + 0x10],EDX
0820a33c e8 df f0        CALL       FUN_08209420
         ff ff
```

Binary: eCh0raix – x86

Statically allocated string structure

Example – before executing the script



```
                      PTR_DAT_08436680                          XREF[2]:     0820a330(*), 08431db0(*)
08436680 e1 85 27 08      addr        DAT_082785e1
08436684 04               ??          04h
08436685 00               ??          00h
08436686 00               ??          00h
08436687 00               ??          00h
08436688 9d               ??          9Dh
08436689 84               ??          84h
0843668a 27               ??          27h
0843668b 08               ??          08h
0843668c 04               ??          04h
0843668d 00               ??          00h
0843668e 00               ??          00h
0843668f 00               ??          00h
08436690 b1               ??          B1h
08436691 84               ??          84h
08436692 27               ??          27h
08436693 08               ??          08h
08436694 04               ??          04h
08436695 00               ??          00h
08436696 00               ??          00h
08436697 00               ??          00h
```

String pointers

String length

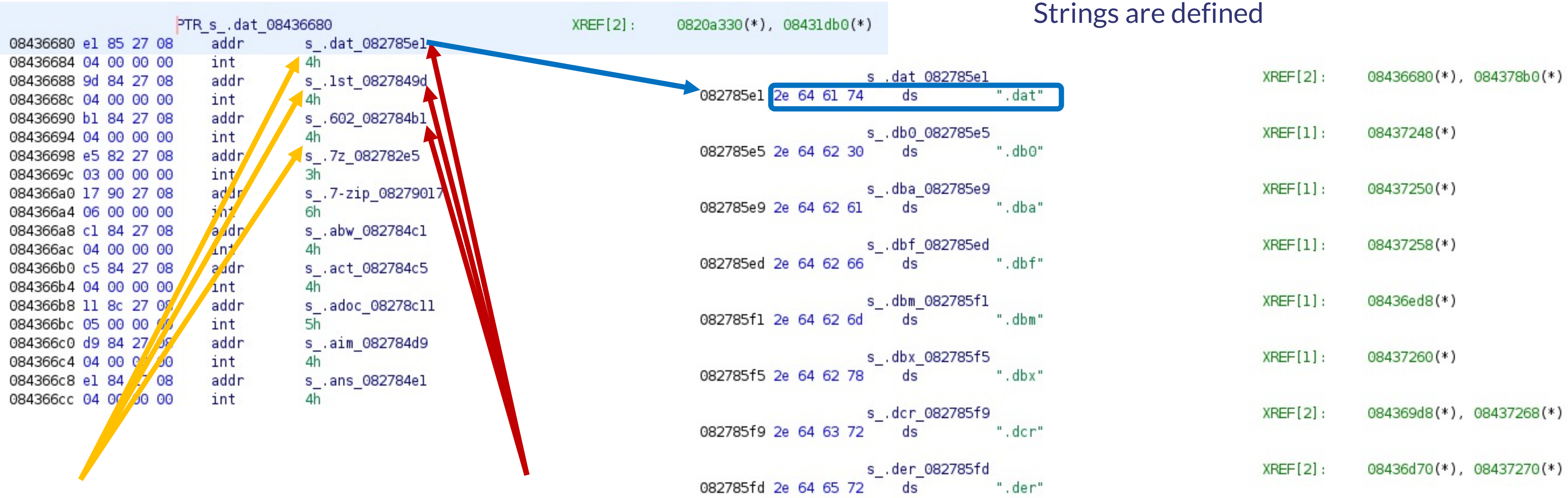
Strings are not defined

```
                DAT_082785e1                                    XREF[1]:     08436680(*)
082785e1 2e          ??        2Eh     .
082785e2 64          ??        64h     d
082785e3 61          ??        61h     a
082785e4 74          ??        74h     t
082785e5 2e          ??        2Eh     .
082785e6 64          ??        64h     d
082785e7 62          ??        62h     b
082785e8 30          ??        30h     0
082785e9 2e          ??        2Eh     .
082785ea 64          ??        64h     d
082785eb 62          ??        62h     b
082785ec 61          ??        61h     a
082785ed 2e          ??        2Eh     .
082785ee 64          ??        64h     d
082785ef 62          ??        62h     b
082785f0 66          ??        66h     f
082785f1 2e          ??        2Eh     .
082785f2 64          ??        64h     d
082785f3 62          ??        62h     b
082785f4 6d          ??        6Dh     m
```

Binary: eCh0raix – x86

Statically allocated string structure

Example – after executing the script



Strings are defined

```
                     PTR_s_.dat_08436680                    XREF[2]:     0820a330(*), 08431db0(*)
08436680 e1 85 27 08     addr       s_.dat_082785e1
08436684 04 00 00 00     int        4h
08436688 9d 84 27 08     addr       s_.1st_0827849d
0843668c 04 00 00 00     int        4h
08436690 b1 84 27 08     addr       s_.602_082784b1
08436694 04 00 00 00     int        4h
08436698 e5 82 27 08     addr       s_.7z_082782e5
0843669c 03 00 00 00     int        3h
084366a0 17 90 27 08     addr       s_.7-zip_08279017
084366a4 06 00 00 00     int        6h
084366a8 c1 84 27 08     addr       s_.abw_082784c1
084366ac 04 00 00 00     int        4h
084366b0 c5 84 27 08     addr       s_.act_082784c5
084366b4 04 00 00 00     int        4h
084366b8 11 8c 27 08     addr       s_.adoc_08278c11
084366bc 05 00 00 00     int        5h
084366c0 d9 84 27 08     addr       s_.aim_082784d9
084366c4 04 00 00 00     int        4h
084366c8 e1 84 27 08     addr       s_.ans_082784e1
084366cc 04 00 00 00     int        4h
```

```
                    s_.dat_082785e1                         XREF[2]:     08436680(*), 084378b0(*)
082785e1 2e 64 61 74     ds          ".dat"

                    s_.db0_082785e5                         XREF[1]:     08437248(*)
082785e5 2e 64 62 30     ds          ".db0"

                    s_.dba_082785e9                         XREF[1]:     08437250(*)
082785e9 2e 64 62 61     ds          ".dba"

                    s_.dbf_082785ed                         XREF[1]:     08437258(*)
082785ed 2e 64 62 66     ds          ".dbf"

                    s_.dbm_082785f1                         XREF[1]:     08436ed8(*)
082785f1 2e 64 62 6d     ds          ".dbm"

                    s_.dbx_082785f5                         XREF[1]:     08437260(*)
082785f5 2e 64 62 78     ds          ".dbx"

                    s_.dcr_082785f9                         XREF[2]:     084369d8(*), 08437268(*)
082785f9 2e 64 63 72     ds          ".dcr"

                    s_.der_082785fd                         XREF[2]:     08436d70(*), 08437270(*)
082785fd 2e 64 65 72     ds          ".der"
```

String length

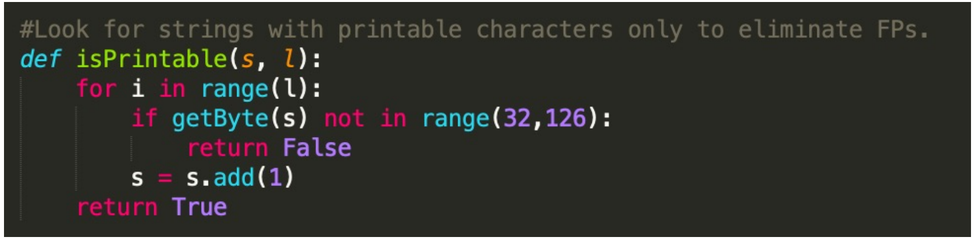
String pointers

Binary: eCh0raix – x86

Statically allocated string structure

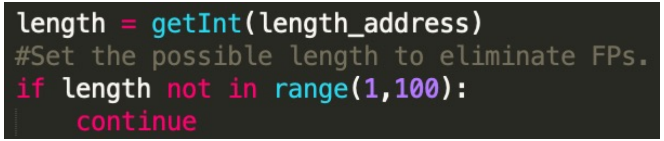
Challenges

- Non-printable characters
    - A string might contain non-printable characters as well (e.g. new line)
    - Experiment with the script, change the values and find the best for your analysis



```
#Look for strings with printable characters only to eliminate FPs.
def isPrintable(s, l):
    for i in range(l):
        if getByte(s) not in range(32,126):
            return False
        s = s.add(1)
    return True
```

- String length limitation
    - Missing some strings
    - Experiment with the script, change the values and find the best for your analysis

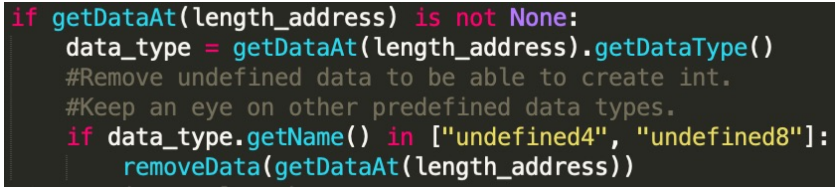


```
length = getInt(length_address)
#Set the possible length to eliminate FPs.
if length not in range(1,100):
    continue
```

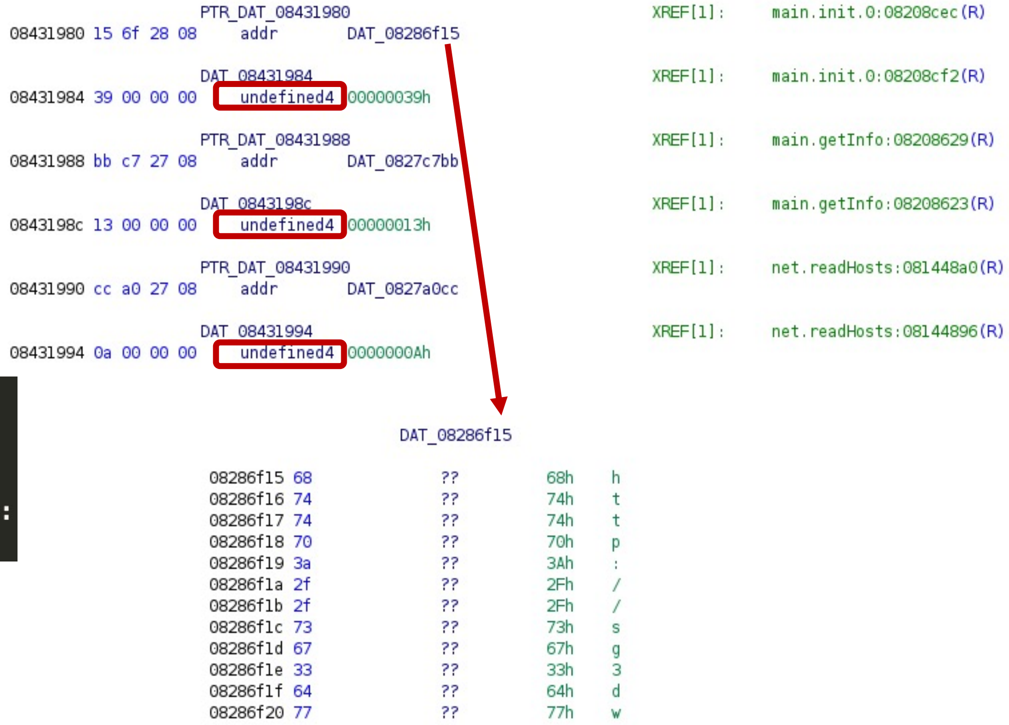
String recovery challenges

Falsely defined data types by Ghidra

- undefined4 or undefined8 (depends on pointer size)
- Already defined data types cannot be redefined
  (undifined4 and undifined8 are defined data types)
- First the data type has to be removed
- Then the new data type can be defined



```python
if getDataAt(length_address) is not None:
    data_type = getDataAt(length_address).getDataType()
    #Remove undefined data to be able to create int.
    #Keep an eye on other predefined data types.
    if data_type.getName() in ["undefined4", "undefined8"]:
        removeData(getDataAt(length_address))
```



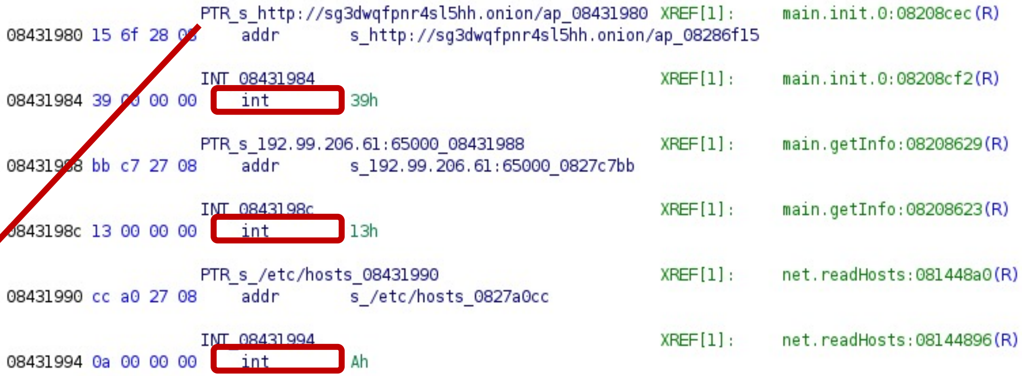
```
                   PTR_DAT_08431980                          XREF[1]:    main.init.0:08208cec(R)
08431980 15 6f 28 08    addr         DAT_08286f15
                   DAT_08431984                              XREF[1]:    main.init.0:08208cf2(R)
08431984 39 00 00 00    undefined4   00000039h
                   PTR_DAT_08431988                          XREF[1]:    main.getInfo:08208629(R)
08431988 bb c7 27 08    addr         DAT_0827c7bb
                   DAT_0843198c                              XREF[1]:    main.getInfo:08208623(R)
0843198c 13 00 00 00    undefined4   00000013h
                   PTR_DAT_08431990                          XREF[1]:    net.readHosts:081448a0(R)
08431990 cc a0 27 08    addr         DAT_0827a0cc
                   DAT_08431994                              XREF[1]:    net.readHosts:08144896(R)
08431994 0a 00 00 00    undefined4   0000000Ah

                          DAT_08286f15

           08286f15 68          ??        68h    h
           08286f16 74          ??        74h    t
           08286f17 74          ??        74h    t
           08286f18 70          ??        70h    p
           08286f19 3a          ??        3Ah    :
           08286f1a 2f          ??        2Fh    /
           08286f1b 2f          ??        2Fh    /
           08286f1c 73          ??        73h    s
           08286f1d 67          ??        67h    g
           08286f1e 33          ??        33h    3
           08286f1f 64          ??        64h    d
           08286f20 77          ??        77h    w
```

Binary: eCh0raix – x86

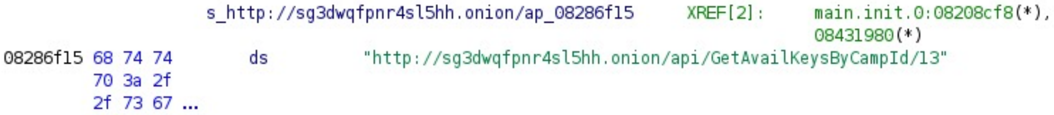
String recovery challenges

Falsely defined data types by Ghidra

- undefined4 or undefined8 (depends on pointer size)
- Already defined data types cannot be redefined
  (undifined4 and undifined8 are defined data types)
- First the data type has to be removed
- Then the new data type can be defined



```
                     PTR_s_http://sg3dwqfpnr4sl5hh.onion/ap_08431980  XREF[1]:     main.init.0:08208cec(R)
08431980 15 6f 28 08     addr       s_http://sg3dwqfpnr4sl5hh.onion/ap_08286f15

                     INT_08431984                                      XREF[1]:     main.init.0:08208cf2(R)
08431984 39 00 00 00     int        39h

                     PTR_s_192.99.206.61:65000_08431988               XREF[1]:     main.getInfo:08208629(R)
08431988 bb c7 27 08     addr       s_192.99.206.61:65000_0827c7bb

                     INT_0843198c                                      XREF[1]:     main.getInfo:08208623(R)
0843198c 13 00 00 00     int        13h

                     PTR_s_/etc/hosts_08431990                         XREF[1]:     net.readHosts:081448a0(R)
08431990 cc a0 27 08     addr       s_/etc/hosts_0827a0cc

                     INT_08431994                                      XREF[1]:     net.readHosts:08144896(R)
08431994 0a 00 00 00     int        Ah
```



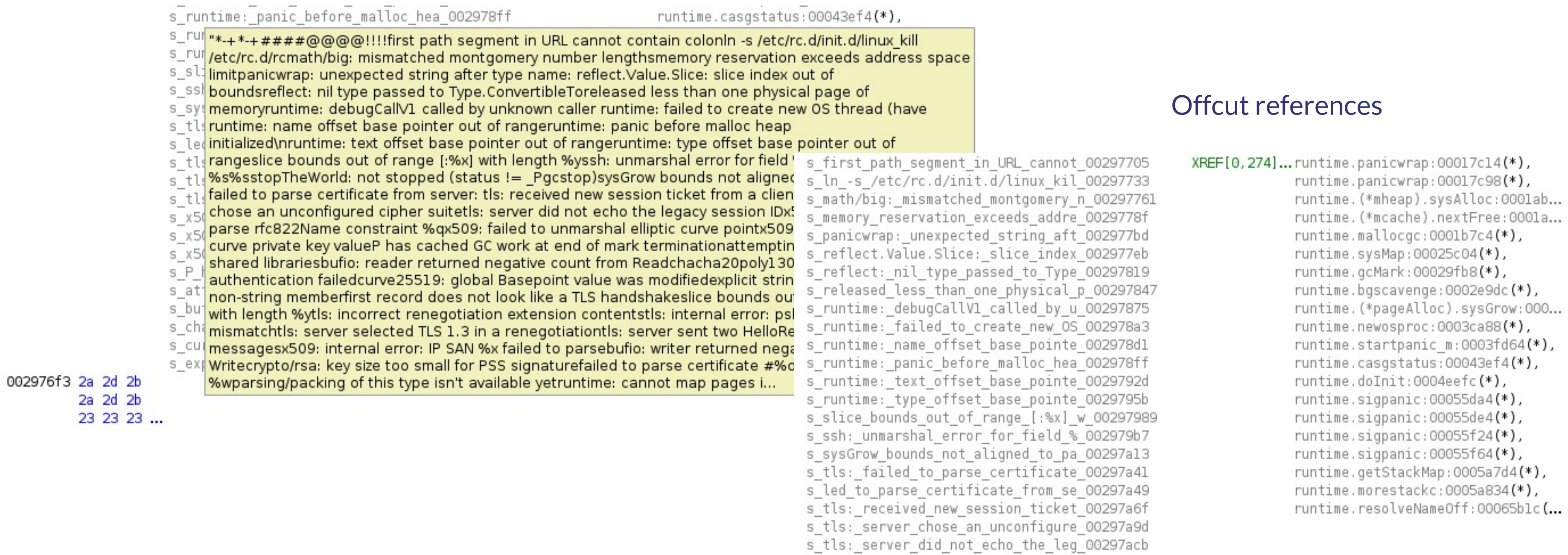
```
                   s_http://sg3dwqfpnr4sl5hh.onion/ap_08286f15      XREF[2]:     main.init.0:08208cf8(*),
                                                                                 08431980(*)
08286f15 68 74 74        ds         "http://sg3dwqfpnr4sl5hh.onion/api/GetAvailKeysByCampId/13"
         70 3a 2f
         2f 73 67 ...
```

Binary: eCh0raix – x86

String recovery challenges

Falsely defined data types by Ghidra

- A large string blob (containing multiple strings) defined as one string



```
s_runtime:_panic_before_malloc_hea_002978ff                runtime.casgstatus:00043ef4(*),

002976f3 2a 2d 2b
         2a 2d 2b
         23 23 23 ...
```

```
"*-+*-+####@@@@!!!!first path segment in URL cannot contain colonln -s /etc/rc.d/init.d/linux_kill
/etc/rc.d/rcmath/big: mismatched montgomery number lengthsmemory reservation exceeds address space
limitpanicwrap: unexpected string after type name: reflect.Value.Slice: slice index out of
boundsreflect: nil type passed to Type.ConvertibleToreleased less than one physical page of
memoryruntime: debugCallV1 called by unknown caller runtime: failed to create new OS thread (have
runtime: name offset base pointer out of rangeruntime: panic before malloc heap
initialized\nruntime: text offset base pointer out of rangeruntime: type offset base pointer out of
rangeslice bounds out of range [:%x] with length %yssh: unmarshal error for field
%s%sstopTheWorld: not stopped (status != _Pgcstop)sysGrow bounds not alignec
failed to parse certificate from server: tls: received new session ticket from a clien
chose an unconfigured cipher suitetls: server did not echo the legacy session IDx
parse rfc822Name constraint %qx509: failed to unmarshal elliptic curve pointx509
curve private key valueP has cached GC work at end of mark terminationattemptin
shared librariesbufio: reader returned negative count from Readchacha20poly130
authentication failedcurve25519: global Basepoint value was modifiedexplicit strin
non-string memberfirst record does not look like a TLS handshakeslice bounds ou
with length %ytls: incorrect renegotiation extension contentstls: internal error: psl
mismatchtls: server selected TLS 1.3 in a renegotiationtls: server sent two HelloRe
messagesx509: internal error: IP SAN %x failed to parsebufio: writer returned nega
Writecrypto/rsa: key size too small for PSS signaturefailed to parse certificate #%c
%wparsing/packing of this type isn't available yetruntime: cannot map pages i...
```

```
s_first_path_segment_in_URL_cannot_00297705
s_ln_-s_/etc/rc.d/init.d/linux_kil_00297733
s_math/big:_mismatched_montgomery_n_00297761
s_memory_reservation_exceeds_addre_0029778f
s_panicwrap:_unexpected_string_aft_002977bd
s_reflect.Value.Slice:_slice_index_002977eb
s_reflect:_nil_type_passed_to_Type_00297819
s_released_less_than_one_physical_p_00297847
s_runtime:_debugCallV1_called_by_u_00297875
s_runtime:_failed_to_create_new_OS_002978a3
s_runtime:_name_offset_base_pointe_002978d1
s_runtime:_panic_before_malloc_hea_002978ff
s_runtime:_text_offset_base_pointe_0029792d
s_runtime:_type_offset_base_pointe_0029795b
s_slice_bounds_out_of_range_[:%x]_w_00297989
s_ssh:_unmarshal_error_for_field_%_002979b7
s_sysGrow_bounds_not_aligned_to_pa_00297a13
s_tls:_failed_to_parse_certificate_00297a41
s_led_to_parse_certificate_from_se_00297a49
s_tls:_received_new_session_ticket_00297a6f
s_tls:_server_chose_an_unconfigure_00297a9d
s_tls:_server_did_not_echo_the_leg_00297acb
```

Offcut references

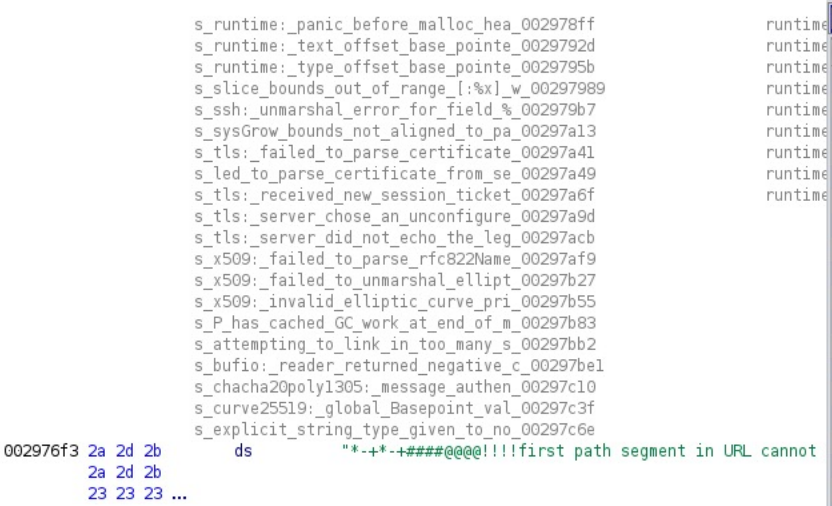
```
XREF[0,274]...runtime.panicwrap:00017c14(*),
              runtime.panicwrap:00017c98(*),
              runtime.(*mheap).sysAlloc:0001ab...
              runtime.(*mcache).nextFree:0001a...
              runtime.mallocgc:0001b7c4(*),
              runtime.sysMap:00025c04(*),
              runtime.gcMark:00029fb8(*),
              runtime.bgscavenge:0002e9dc(*),
              runtime.(*pageAlloc).sysGrow:000...
              runtime.newosproc:0003ca88(*),
              runtime.startpanic_m:0003fd64(*),
              runtime.casgstatus:00043ef4(*),
              runtime.doInit:0004eefc(*),
              runtime.sigpanic:00055da4(*),
              runtime.sigpanic:00055de4(*),
              runtime.sigpanic:00055f24(*),
              runtime.sigpanic:00055f64(*),
              runtime.getStackMap:0005a7d4(*),
              runtime.morestackc:0005a834(*),
              runtime.resolveNameOff:00065b1c(...
```

Binary: Kaiji – ARM

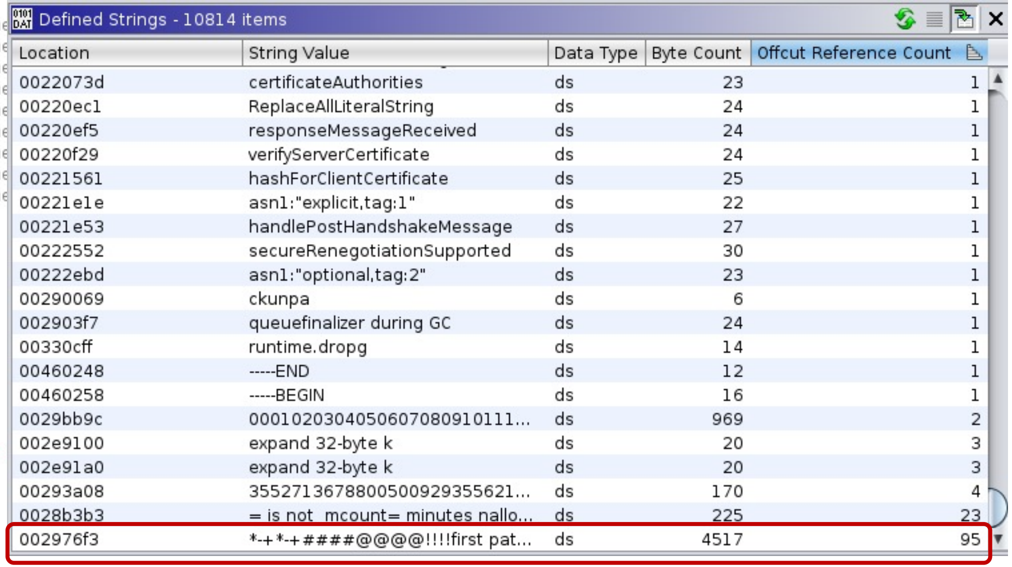
String recovery challenges

Falsely defined data types by Ghidra

- A large string blob (containing multiple strings) defined as one string



```
                  s_runtime:_panic_before_malloc_hea_002978ff                runtime
                  s_runtime:_text_offset_base_pointe_0029792d                runtime
                  s_runtime:_type_offset_base_pointe_0029795b                runtime
                  s_slice_bounds_out_of_range_[:%x]_w_00297989               runtime
                  s_ssh:_unmarshal_error_for_field_%_002979b7                runtime
                  s_sysGrow_bounds_not_aligned_to_pa_00297a13                runtime
                  s_tls:_failed_to_parse_certificate_00297a41                runtime
                  s_led_to_parse_certificate_from_se_00297a49                runtime
                  s_tls:_received_new_session_ticket_00297a6f                runtime
                  s_tls:_server_chose_an_unconfigure_00297a9d
                  s_tls:_server_did_not_echo_the_leg_00297acb
                  s_x509:_failed_to_parse_rfc822Name_00297af9
                  s_x509:_failed_to_unmarshal_ellipt_00297b27
                  s_x509:_invalid_elliptic_curve_pri_00297b55
                  s_P_has_cached_GC_work_at_end_of_m_00297b83
                  s_attempting_to_link_in_too_many_s_00297bb2
                  s_bufio:_reader_returned_negative_c_00297be1
                  s_chacha20poly1305:_message_authen_00297c10
                  s_curve25519:_global_Basepoint_val_00297c3f
                  s_explicit_string_type_given_to_no_00297c6e
002976f3 2a 2d 2b      ds        "*-+*-+####@@@@!!!!first path segment in URL cannot
         2a 2d 2b
         23 23 23 ...
```



Defined Strings - 10814 items

Location	String Value	Data Type	Byte Count	Offcut Reference Count
0022073d	certificateAuthorities	ds	23	1
00220ec1	ReplaceAllLiteralString	ds	24	1
00220ef5	responseMessageReceived	ds	24	1
00220f29	verifyServerCertificate	ds	24	1
00221561	hashForClientCertificate	ds	25	1
00221e1e	asn1:"explicit,tag:1"	ds	22	1
00221e53	handlePostHandshakeMessage	ds	27	1
00222552	secureRenegotiationSupported	ds	30	1
00222ebd	asn1:"optional,tag:2"	ds	23	1
00290069	ckunpa	ds	6	1
002903f7	queuefinalizer during GC	ds	24	1
00330cff	runtime.dropg	ds	14	1
00460248	-----END	ds	12	1
00460258	-----BEGIN	ds	16	1
0029bb9c	0001020304050607080910111...	ds	969	2
002e9100	expand 32-byte k	ds	20	3
002e91a0	expand 32-byte k	ds	20	3
00293a08	3552713678800500929355621...	ds	170	4
0028b3b3	= is not mcount= minutes nallo...	ds	225	23
002976f3	*-+*-+####@@@@!!!!first pat...	ds	4517	95

Binary: Kaiji – ARM

Other researcher’s work

Links

IDA Pro

- https://github.com/sibears/IDAGolangHelper
- https://github.com/strazzere/golang_loader_assist

radare2 / Cutter

- https://github.com/f0rki/r2-go-helpers
- https://github.com/JacobPimental/r2-gohelper/blob/master/golang_helper.py
- https://github.com/CarveSystems/gostringsr2

Binary Ninja

- https://github.com/f0rki/bn-goloader

Ghidra

- https://github.com/felberj/gotools
  Only handles linux/x86_64 binaries.
- https://github.com/ghidraninja/ghidra_scripts/blob/master/golang_renamer.py

Files used during the presentation

Hashes

File name	SHA-256
world.c	761301bb14ea3b678650fc1b6da768f009387ee726712e291d57e2d7985613d0
world.go	7cb3316a7b89eb996e8dbb0d0fb277136cd588cc54642f3b09aa84cd177cb3a2
world_c	76a5c4ef9277b97660f2c412e67ff2c3826e699913db86cd333e8f1d4fb5b8a3
world_c_strip	486a93362a6a8bc3b449fd6ba07656011c687ed31a19091c329a434bff4d75bb
world_go	d0d4781de4ffd5fbe18d59328eccd373a782eecdf55a2c5199b7dc6598cfb99e
world_go_strip	9b975bd9406a8b79a414195e184be0c82bb1593979577f0344c797f9bcd4ad0b
world_go.exe	9e36291f5fc67fdb9e5e17b636d34b39f2cc39f328916a9012a8f8d545e9d0c8
world_go_strip.exe	c5b66623942a0cea6df30541e92afe93172be7bb4dbdd42a1fa354e9edd79a1d
world_go_println	fa00f5ad2aa79a6245a28516bc285ae8c36f075d818787aadff6f3e850e2ec5c
eCh0raix - x86	154dea7cace3d58c0ceccb5a3b8d7e0347674a0e76daffa9fa53578c036d9357
eCh0raix - ARM	3d7ebe73319a3435293838296fbb86c2e920fd0ccc9169285cc2c4d7fa3f120d
Kaiji - x86_64	f4a64ab3ffc0b4a94fd07a55565f24915b7a1aaec58454df5e47d8f8a2eec22a
Kaiji - ARM	3e68118ad46b9eb64063b259fca5f6682c5c2cb18fd9a4e7d97969226b2e6fb4

References, additional reading

Other Go malware research

- https://rednaga.io/2016/09/21/reversing_go_binaries_like_a_pro/
- https://2016.zeronights.ru/wp-content/uploads/2016/12/GO_Zaytsev.pdf
- https://carvesystems.com/news/reverse-engineering-go-binaries-using-radare-2-and-python/
- https://www.pnfsoftware.com/blog/analyzing-golang-executables/
- https://github.com/strazzere/golang_loader_assist/blob/master/Bsides-GO-Forth-And-Reverse.pdf
- https://github.com/radareorg/r2con2020/blob/master/day2/r2_Gophers-AnalysisOfGoBinariesWithRadare2.pdf

VB2021 localhost
October 2021

Dorka Palotay
Senior Threat Researcher, CUJO AI
@pad0rka

Albert Zsigovits
Threat Researcher, CUJO AI
@albertzsigovits

CUJO AI Labs
https://github.com/getCUJO/ThreatIntel
@CujoaiLabs