# CSAW Debrief
# Gopherz Reversing

By Sam Williams

# Who Am I?

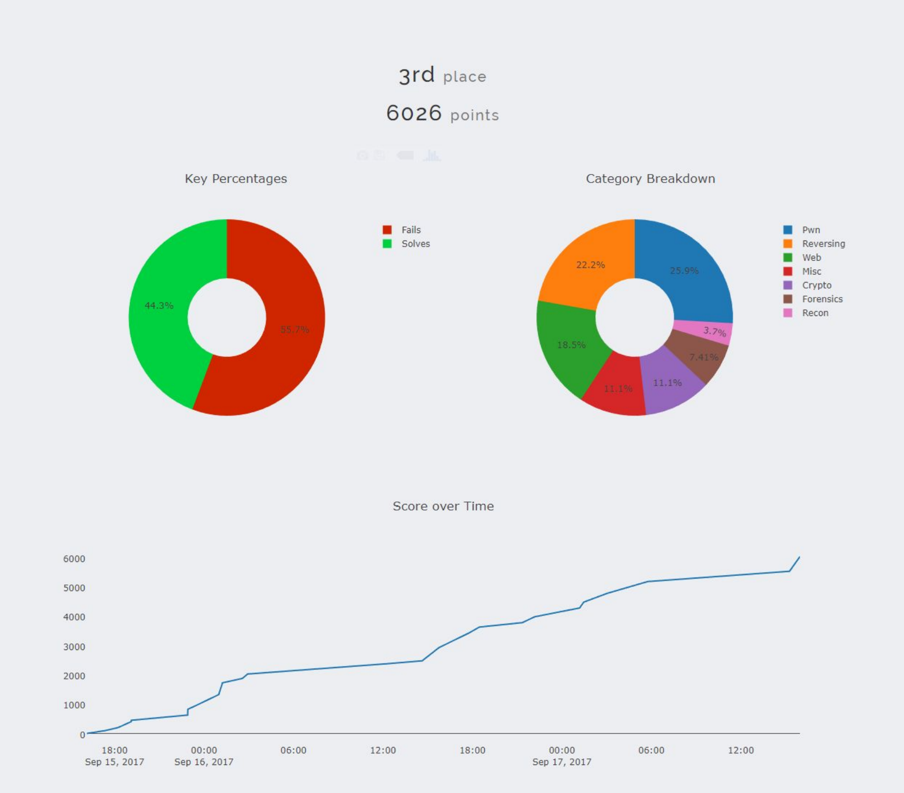
- 6 years doing professional Vulnerability Research and Security development
- ~8 Years playing CTF
  - WCSC
  - Hates Irony
  - Ghost in the Shellcode
  - (mostly) Men in Black Hats
  - Mammon Machine
  - Nasa Rejects ⇐ Current
- Stream security topics weekly (although typically during these meetings)
  - Currently doing bug finding in Windows 95/IE 5.5
  - ▶ / 🐦 MurmusCTF

# What is CSAW?

- Yearly competition
- Run by NYU Poly
- Long running event (14th conference)
- Qualifying round typically in September, open to everyone
- Final, in person event typically in November, open to undergrad teams

# NASA Rejects playing CSAW

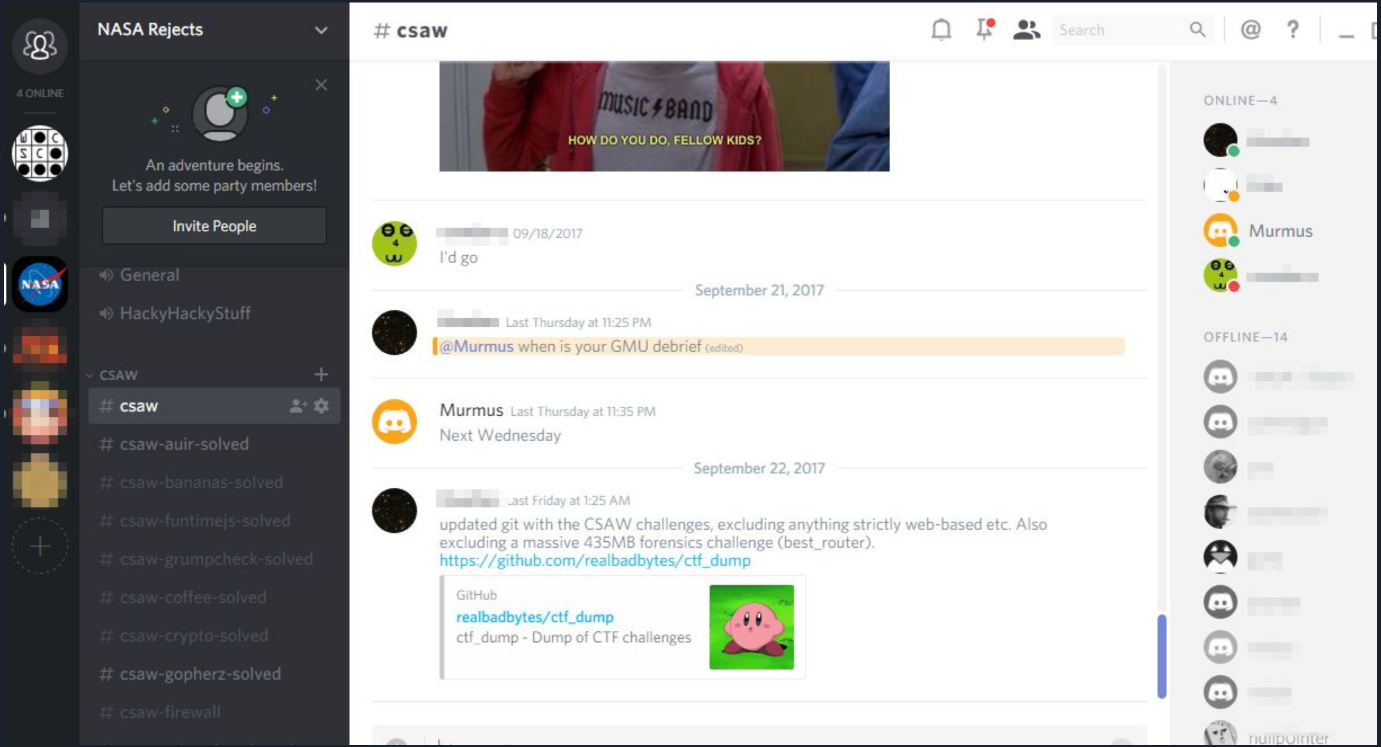
- Distributed team (~8 active players, played from at least 4 states)
- Most of us have worked together previously and since moved on to new things



3rd place

6026 points

# Staying Organized



[redacted] 09/18/2017
I'd go

September 21, 2017

[redacted] Last Thursday at 11:25 PM
@Murmus when is your GMU debrief (edited)

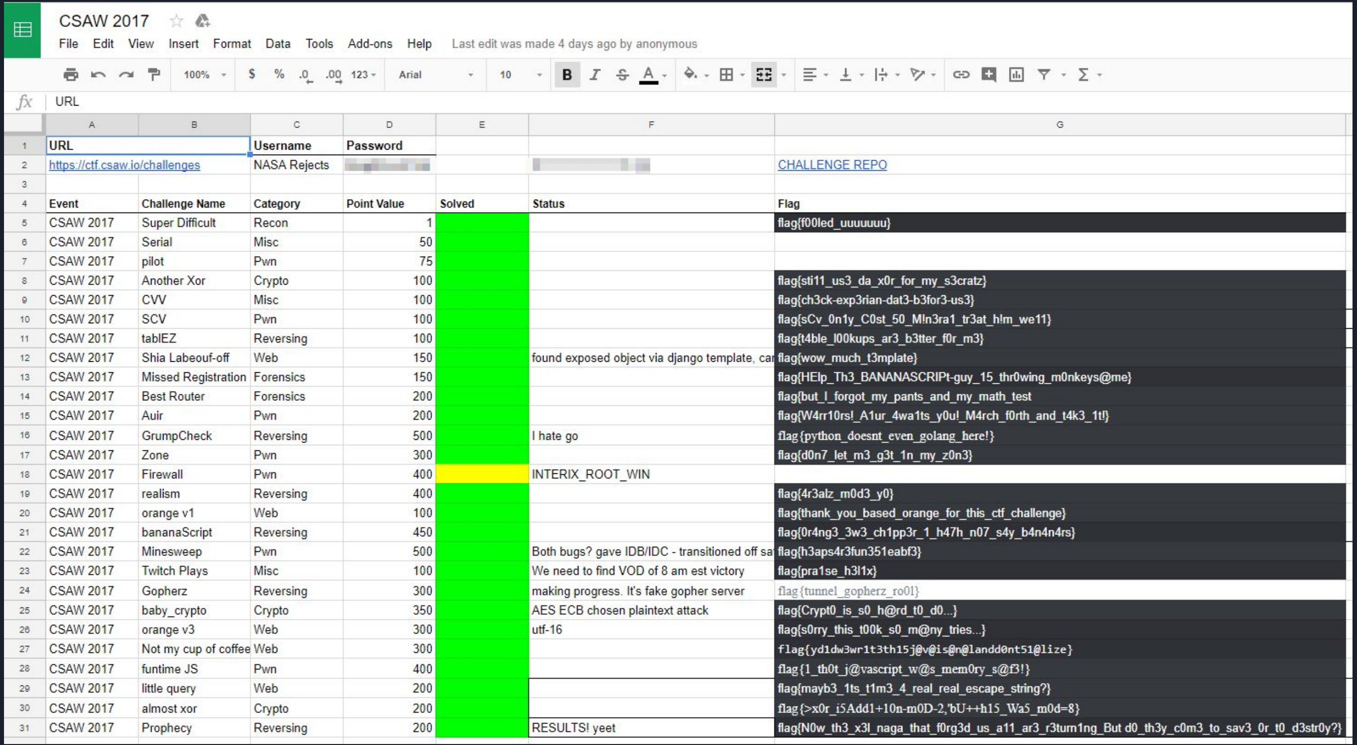
Murmus Last Thursday at 11:35 PM
Next Wednesday

September 22, 2017

[redacted] Last Friday at 1:25 AM
updated git with the CSAW challenges, excluding anything strictly web-based etc. Also excluding a massive 435MB forensics challenge (best_router).
https://github.com/realbadbytes/ctf_dump

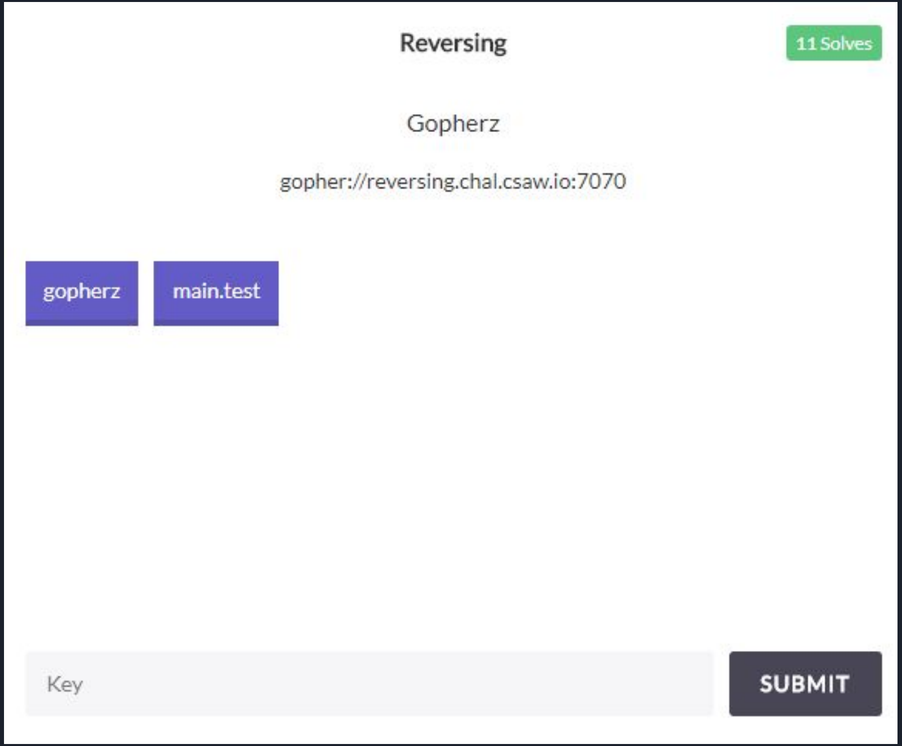
GitHub
realbadbytes/ctf_dump
ctf_dump - Dump of CTF challenges

# Staying Organized Cont.



| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | URL | | Username | Password | | | |
| 2 | https://ctf.csaw.io/challenges | | NASA Rejects | [redacted] | | [redacted] | CHALLENGE REPO |
| 3 | | | | | | | |
| 4 | Event | Challenge Name | Category | Point Value | Solved | Status | Flag |
| 5 | CSAW 2017 | Super Difficult | Recon | 1 | 🟩 | | flag{f00led_uuuuuuu} |
| 6 | CSAW 2017 | Serial | Misc | 50 | 🟩 | | |
| 7 | CSAW 2017 | pilot | Pwn | 75 | 🟩 | | |
| 8 | CSAW 2017 | Another Xor | Crypto | 100 | 🟩 | | flag{sti11_us3_da_x0r_for_my_s3cratz} |
| 9 | CSAW 2017 | CVV | Misc | 100 | 🟩 | | flag{ch3ck-exp3rian-dat3-b3for3-us3} |
| 10 | CSAW 2017 | SCV | Pwn | 100 | 🟩 | | flag{sCv_0n1y_C0st_50_M!n3ra1_tr3at_h!m_we11} |
| 11 | CSAW 2017 | tablEZ | Reversing | 100 | 🟩 | | flag{t4ble_l00kups_ar3_b3tter_f0r_m3} |
| 12 | CSAW 2017 | Shia Labeouf-off | Web | 150 | 🟩 | found exposed object via django template, car | flag{wow_much_t3mplate} |
| 13 | CSAW 2017 | Missed Registration | Forensics | 150 | 🟩 | | flag{HElp_Th3_BANANASCRIPt-guy_15_thr0wing_m0nkeys@me} |
| 14 | CSAW 2017 | Best Router | Forensics | 200 | 🟩 | | flag{but_I_forgot_my_pants_and_my_math_test |
| 15 | CSAW 2017 | Auir | Pwn | 200 | 🟩 | | flag{W4rr10rs!_A1ur_4wa1ts_y0u!_M4rch_f0rth_and_t4k3_1t!} |
| 16 | CSAW 2017 | GrumpCheck | Reversing | 500 | 🟩 | I hate go | flag{python_doesnt_even_golang_here!} |
| 17 | CSAW 2017 | Zone | Pwn | 300 | 🟩 | | flag{d0n7_let_m3_g3t_1n_my_z0n3} |
| 18 | CSAW 2017 | Firewall | Pwn | 400 | 🟨 | INTERIX_ROOT_WIN | |
| 19 | CSAW 2017 | realism | Reversing | 400 | 🟩 | | flag{4r3alz_m0d3_y0} |
| 20 | CSAW 2017 | orange v1 | Web | 100 | 🟩 | | flag{thank_you_based_orange_for_this_ctf_challenge} |
| 21 | CSAW 2017 | bananaScript | Reversing | 450 | 🟩 | | flag{0r4ng3_3w3_ch1pp3r_1_h47h_n07_s4y_b4n4n4rs} |
| 22 | CSAW 2017 | Minesweep | Pwn | 500 | 🟩 | Both bugs? gave IDB/IDC - transitioned off sa | flag{h3aps4r3fun351eabf3} |
| 23 | CSAW 2017 | Twitch Plays | Misc | 100 | 🟩 | We need to find VOD of 8 am est victory | flag{pra1se_h3l1x} |
| 24 | CSAW 2017 | Gopherz | Reversing | 300 | 🟩 | making progress. It's fake gopher server | flag{tunnel_gopherz_ro01} |
| 25 | CSAW 2017 | baby_crypto | Crypto | 350 | 🟩 | AES ECB chosen plaintext attack | flag{Crypt0_is_s0_h@rd_t0_d0...} |
| 26 | CSAW 2017 | orange v3 | Web | 300 | 🟩 | utf-16 | flag{s0rry_this_t00k_s0_m@ny_tries...} |
| 27 | CSAW 2017 | Not my cup of coffee | Web | 300 | 🟩 | | flag{yd1dw3wr1t3th15j@v@is@n@landd0nt51@lize} |
| 28 | CSAW 2017 | funtime JS | Pwn | 400 | 🟩 | | flag{1_th0t_j@vascript_w@s_mem0ry_s@f3!} |
| 29 | CSAW 2017 | little query | Web | 200 | 🟩 | | flag{mayb3_1ts_t1m3_4_real_real_escape_string?} |
| 30 | CSAW 2017 | almost xor | Crypto | 200 | 🟩 | | flag{>x0r_i5Add1+10n-m0D-2,'bU++h15_Wa5_m0d=8} |
| 31 | CSAW 2017 | Prophecy | Reversing | 200 | 🟩 | RESULTS! yeet | flag{N0w_th3_x3l_naga_that_f0rg3d_us_a11_ar3_r3turn1ng_But d0_th3y_c0m3_to_sav3_0r_t0_d3str0y?} |

# Gopherz

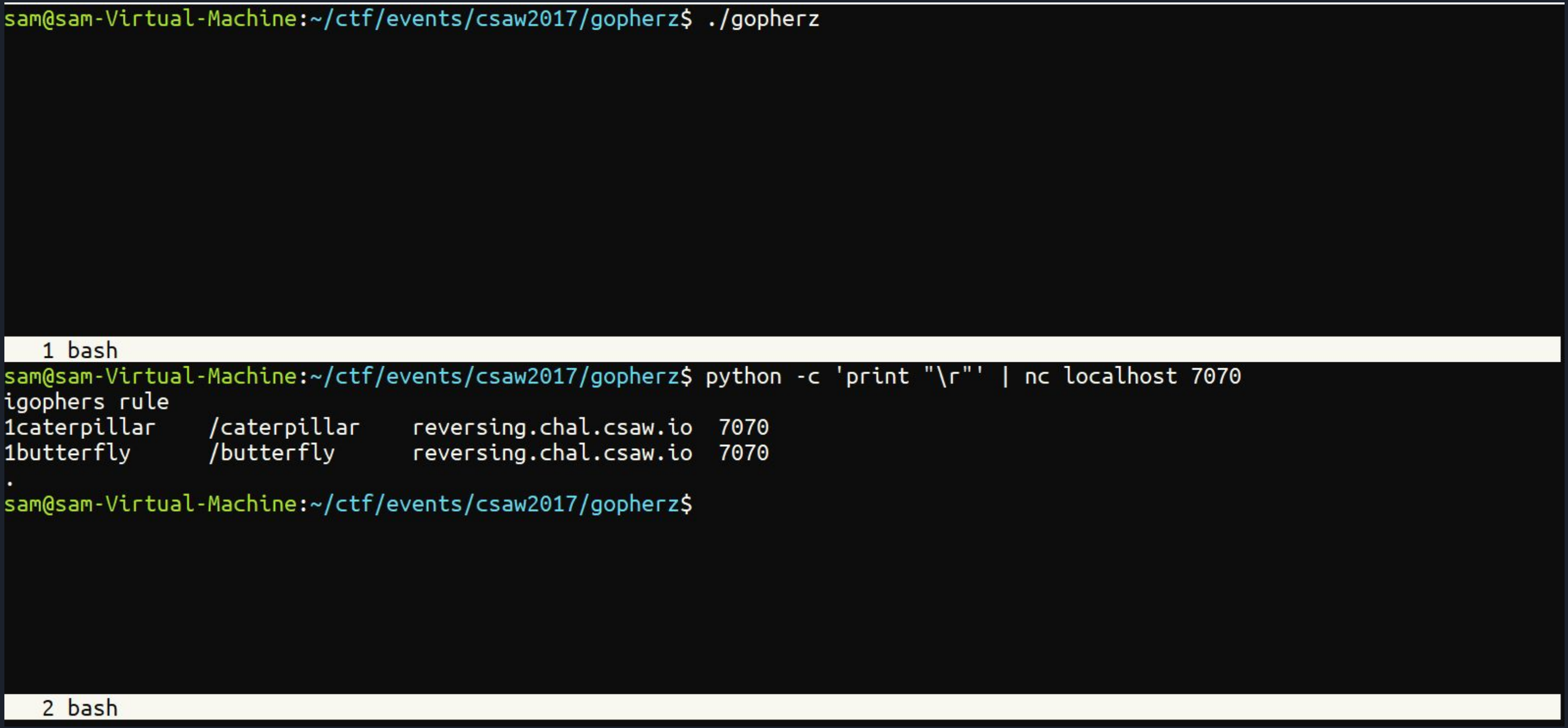


Reversing

Gopherz

gopher://reversing.chal.csaw.io:7070

# Basic Interaction



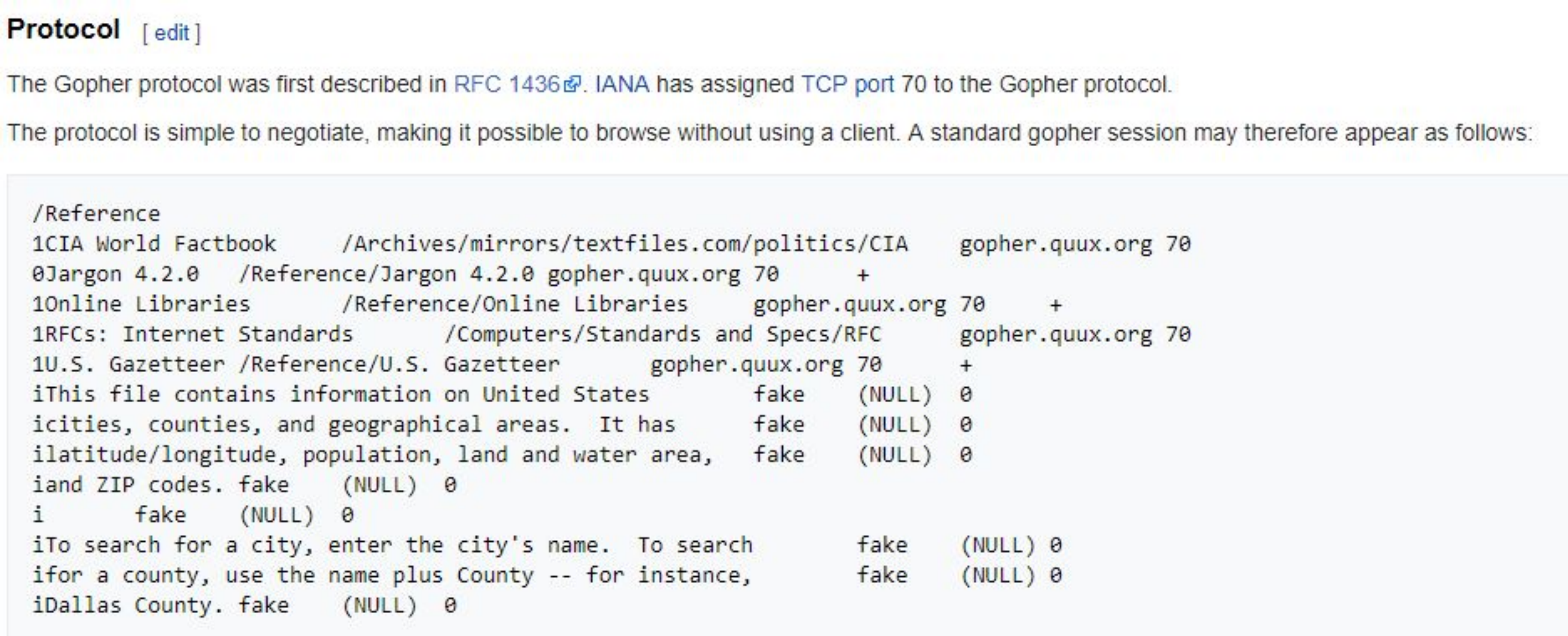
```
sam@sam-Virtual-Machine:~/ctf/events/csaw2017/gopherz$ ./gopherz
```

```
  1 bash
```

```
sam@sam-Virtual-Machine:~/ctf/events/csaw2017/gopherz$ python -c 'print "\r"' | nc localhost 7070
igophers rule
1caterpillar    /caterpillar    reversing.chal.csaw.io  7070
1butterfly      /butterfly      reversing.chal.csaw.io  7070
.
sam@sam-Virtual-Machine:~/ctf/events/csaw2017/gopherz$
```

```
  2 bash
```

# Gopher Protocol



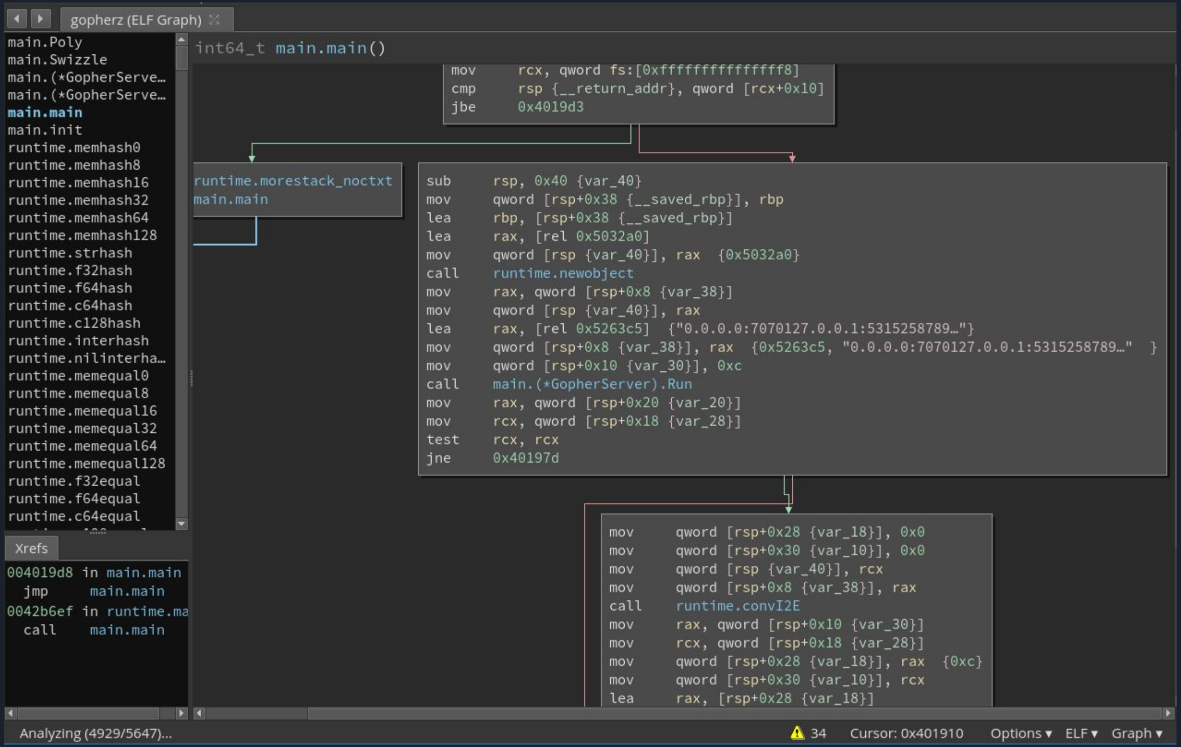
## Protocol [ edit ]

The Gopher protocol was first described in RFC 1436. IANA has assigned TCP port 70 to the Gopher protocol.

The protocol is simple to negotiate, making it possible to browse without using a client. A standard gopher session may therefore appear as follows:

```
/Reference
1CIA World Factbook     /Archives/mirrors/textfiles.com/politics/CIA    gopher.quux.org 70
0Jargon 4.2.0   /Reference/Jargon 4.2.0 gopher.quux.org 70      +
1Online Libraries       /Reference/Online Libraries     gopher.quux.org 70      +
1RFCs: Internet Standards       /Computers/Standards and Specs/RFC      gopher.quux.org 70
1U.S. Gazetteer /Reference/U.S. Gazetteer       gopher.quux.org 70      +
iThis file contains information on United States        fake    (NULL)  0
icities, counties, and geographical areas.  It has      fake    (NULL)  0
ilatitude/longitude, population, land and water area,   fake    (NULL)  0
iand ZIP codes. fake    (NULL)  0
i       fake    (NULL)  0
iTo search for a city, enter the city's name.  To search        fake    (NULL) 0
ifor a county, use the name plus County -- for instance,        fake    (NULL) 0
iDallas County. fake    (NULL)  0
```

# Disassembly



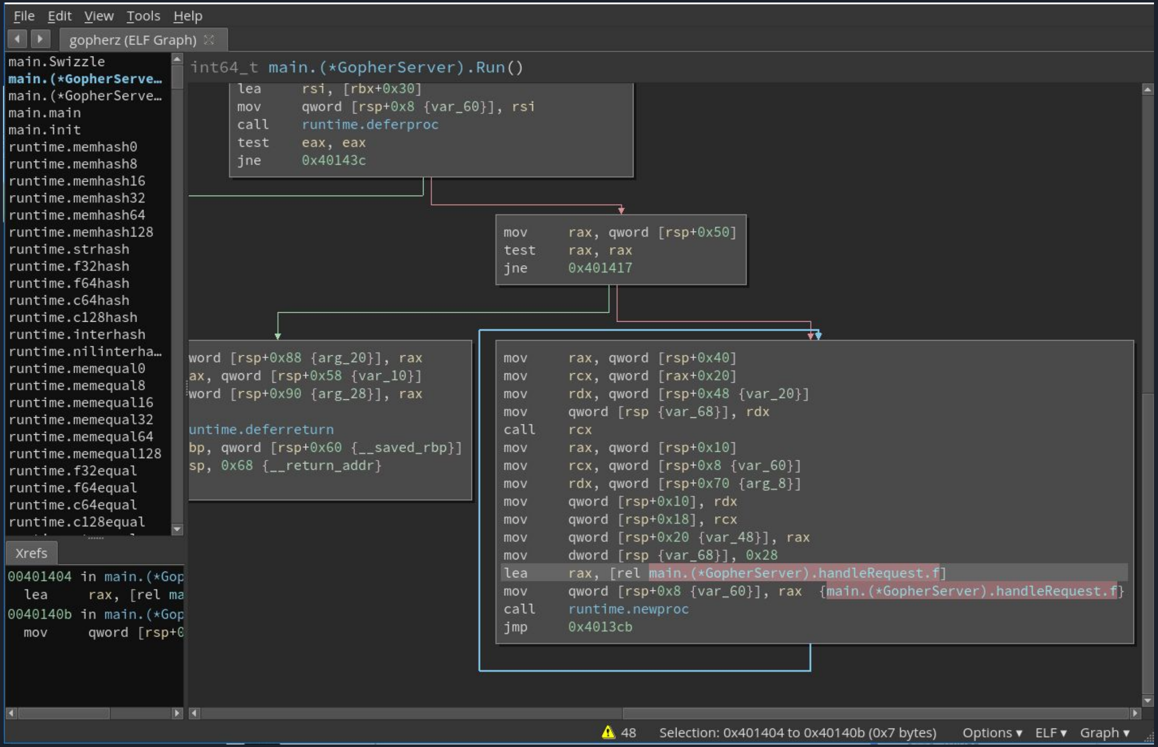
```
main.Poly
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
```

```
004019d8 in main.main
  jmp      main.main
0042b6ef in runtime.ma
  call     main.main
```

```
int64_t main.main()

mov     rcx, qword fs:[0xfffffffffffffff8]
cmp     rsp {__return_addr}, qword [rcx+0x10]
jbe     0x4019d3

runtime.morestack_noctxt
main.main

sub     rsp, 0x40 {var_40}
mov     qword [rsp+0x38 {__saved_rbp}], rbp
lea     rbp, [rsp+0x38 {__saved_rbp}]
lea     rax, [rel 0x5032a0]
mov     qword [rsp {var_40}], rax  {0x5032a0}
call    runtime.newobject
mov     rax, qword [rsp+0x8 {var_38}]
mov     qword [rsp {var_40}], rax
lea     rax, [rel 0x5263c5]  {"0.0.0.0:7070127.0.0.1:5315258789…"}
mov     qword [rsp+0x8 {var_38}], rax  {0x5263c5, "0.0.0.0:7070127.0.0.1:5315258789…"  }
mov     qword [rsp+0x10 {var_30}], 0xc
call    main.(*GopherServer).Run
mov     rax, qword [rsp+0x20 {var_20}]
mov     rcx, qword [rsp+0x18 {var_28}]
test    rcx, rcx
jne     0x40197d

mov     qword [rsp+0x28 {var_18}], 0x0
mov     qword [rsp+0x30 {var_10}], 0x0
mov     qword [rsp {var_40}], rcx
mov     qword [rsp+0x8 {var_38}], rax
call    runtime.convI2E
mov     rax, qword [rsp+0x10 {var_30}]
mov     rcx, qword [rsp+0x18 {var_28}]
mov     qword [rsp+0x28 {var_18}], rax  {0xc}
mov     qword [rsp+0x30 {var_10}], rcx
lea     rax, [rsp+0x28 {var_18}]
```

```
Analyzing (4929/5647)...    ⚠ 34    Cursor: 0x401910
```

# Disassembly



```
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
runtime.c128equal
```

```
int64_t main.(*GopherServer).Run()
```

```
lea     rsi, [rbx+0x30]
mov     qword [rsp+0x8 {var_60}], rsi
call    runtime.deferproc
test    eax, eax
jne     0x40143c
```

```
mov     rax, qword [rsp+0x50]
test    rax, rax
jne     0x401417
```

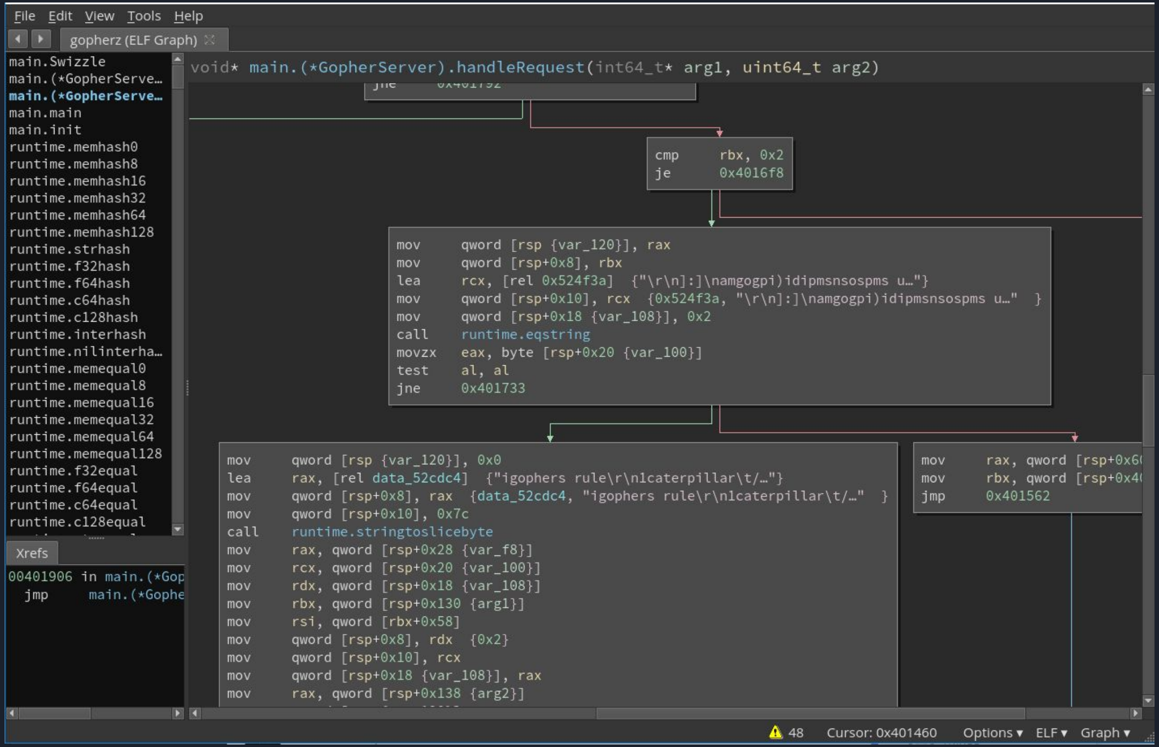
```
word [rsp+0x88 {arg_20}], rax
ax, qword [rsp+0x58 {var_10}]
word [rsp+0x90 {arg_28}], rax

untime.deferreturn
bp, qword [rsp+0x60 {__saved_rbp}]
sp, 0x68 {__return_addr}
```

```
mov     rax, qword [rsp+0x40]
mov     rcx, qword [rax+0x20]
mov     rdx, qword [rsp+0x48 {var_20}]
mov     qword [rsp {var_68}], rdx
call    rcx
mov     rax, qword [rsp+0x10]
mov     rcx, qword [rsp+0x8 {var_60}]
mov     rdx, qword [rsp+0x70 {arg_8}]
mov     qword [rsp+0x10], rdx
mov     qword [rsp+0x18], rcx
mov     qword [rsp+0x20 {var_48}], rax
mov     dword [rsp {var_68}], 0x28
lea     rax, [rel main.(*GopherServer).handleRequest.f]
mov     qword [rsp+0x8 {var_60}], rax  {main.(*GopherServer).handleRequest.f}
call    runtime.newproc
jmp     0x4013cb
```

```
00401404 in main.(*Gop
  lea     rax, [rel ma
0040140b in main.(*Gop
  mov     qword [rsp+0
```

⚠ 48   Selection: 0x401404 to 0x40140b (0x7 bytes)

# Disassembly

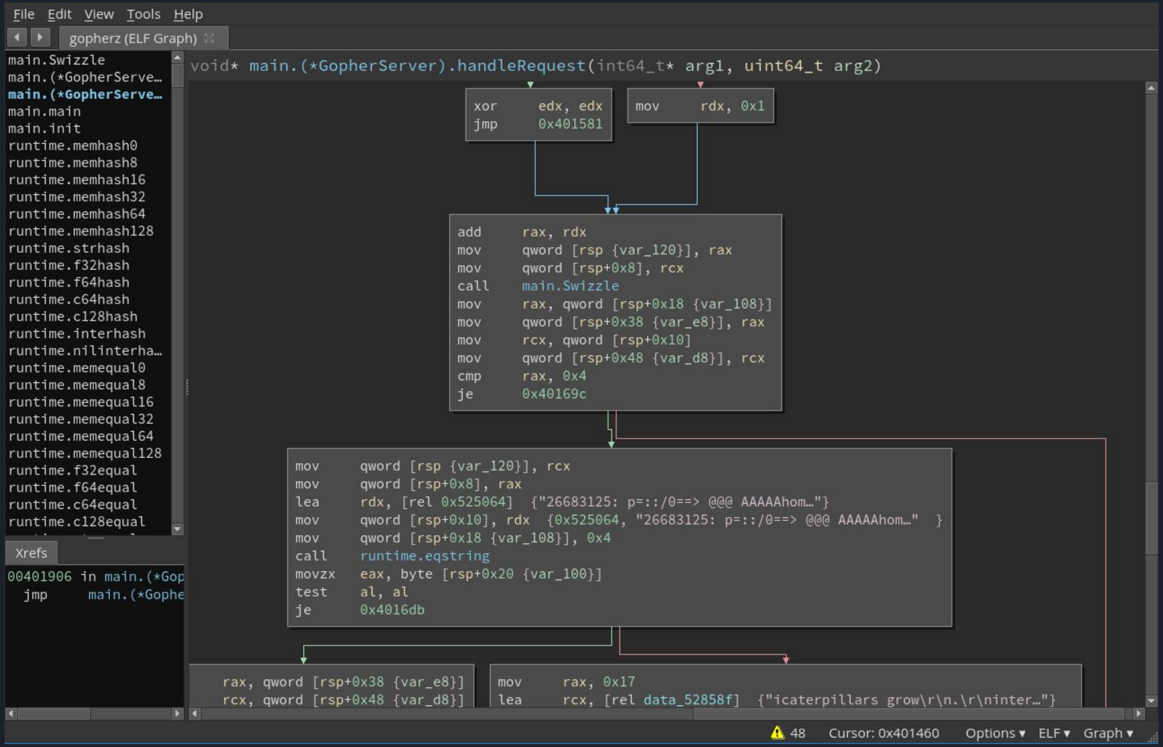


```
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
runtime.c128equal
```

```
00401906 in main.(*Gop
  jmp      main.(*Gophe
```

```
void* main.(*GopherServer).handleRequest(int64_t* arg1, uint64_t arg2)

jne     0x401792

cmp     rbx, 0x2
je      0x4016f8

mov     qword [rsp {var_120}], rax
mov     qword [rsp+0x8], rbx
lea     rcx, [rel 0x524f3a]  {"\r\n]:]\namgogpi)idipmsnsospms u…"}
mov     qword [rsp+0x10], rcx  {0x524f3a, "\r\n]:]\namgogpi)idipmsnsospms u…"  }
mov     qword [rsp+0x18 {var_108}], 0x2
call    runtime.eqstring
movzx   eax, byte [rsp+0x20 {var_100}]
test    al, al
jne     0x401733

mov     qword [rsp {var_120}], 0x0
lea     rax, [rel data_52cdc4]  {"igophers rule\r\n1caterpillar\t/…"}
mov     qword [rsp+0x8], rax  {data_52cdc4, "igophers rule\r\n1caterpillar\t/…"  }
mov     qword [rsp+0x10], 0x7c
call    runtime.stringtoslicebyte
mov     rax, qword [rsp+0x28 {var_f8}]
mov     rcx, qword [rsp+0x20 {var_100}]
mov     rdx, qword [rsp+0x18 {var_108}]
mov     rbx, qword [rsp+0x130 {arg1}]
mov     rsi, qword [rbx+0x58]
mov     qword [rsp+0x8], rdx  {0x2}
mov     qword [rsp+0x10], rcx
mov     qword [rsp+0x18 {var_108}], rax
mov     rax, qword [rsp+0x138 {arg2}]

mov     rax, qword [rsp+0x6
mov     rbx, qword [rsp+0x4
jmp     0x401562
```

# Disassembly



```
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
runtime.c128equal
```

```
00401906 in main.(*Gop
  jmp      main.(*Gophe
```

```
void* main.(*GopherServer).handleRequest(int64_t* arg1, uint64_t arg2)
```

```
xor     edx, edx
jmp     0x401581
```

```
mov     rdx, 0x1
```

```
add     rax, rdx
mov     qword [rsp {var_120}], rax
mov     qword [rsp+0x8], rcx
call    main.Swizzle
mov     rax, qword [rsp+0x18 {var_108}]
mov     qword [rsp+0x38 {var_e8}], rax
mov     rcx, qword [rsp+0x10]
mov     qword [rsp+0x48 {var_d8}], rcx
cmp     rax, 0x4
je      0x40169c
```

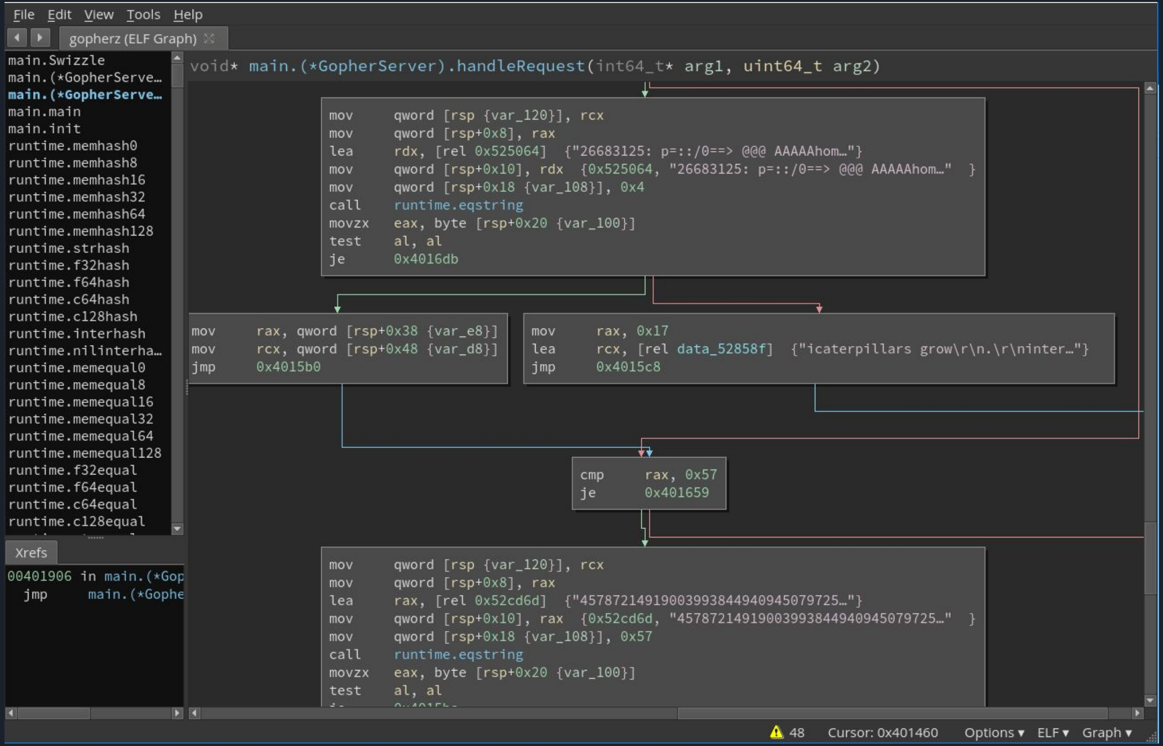
```
mov     qword [rsp {var_120}], rcx
mov     qword [rsp+0x8], rax
lea     rdx, [rel 0x525064]  {"26683125: p=::/0==> @@@ AAAAAhom…"}
mov     qword [rsp+0x10], rdx  {0x525064, "26683125: p=::/0==> @@@ AAAAAhom…"  }
mov     qword [rsp+0x18 {var_108}], 0x4
call    runtime.eqstring
movzx   eax, byte [rsp+0x20 {var_100}]
test    al, al
je      0x4016db
```

```
        rax, qword [rsp+0x38 {var_e8}]
        rcx, qword [rsp+0x48 {var_d8}]
```

```
mov     rax, 0x17
lea     rcx, [rel data_52858f]  {"icaterpillars grow\r\n.\r\ninter…"}
```

⚠ 48    Cursor: 0x401460

# Disassembly

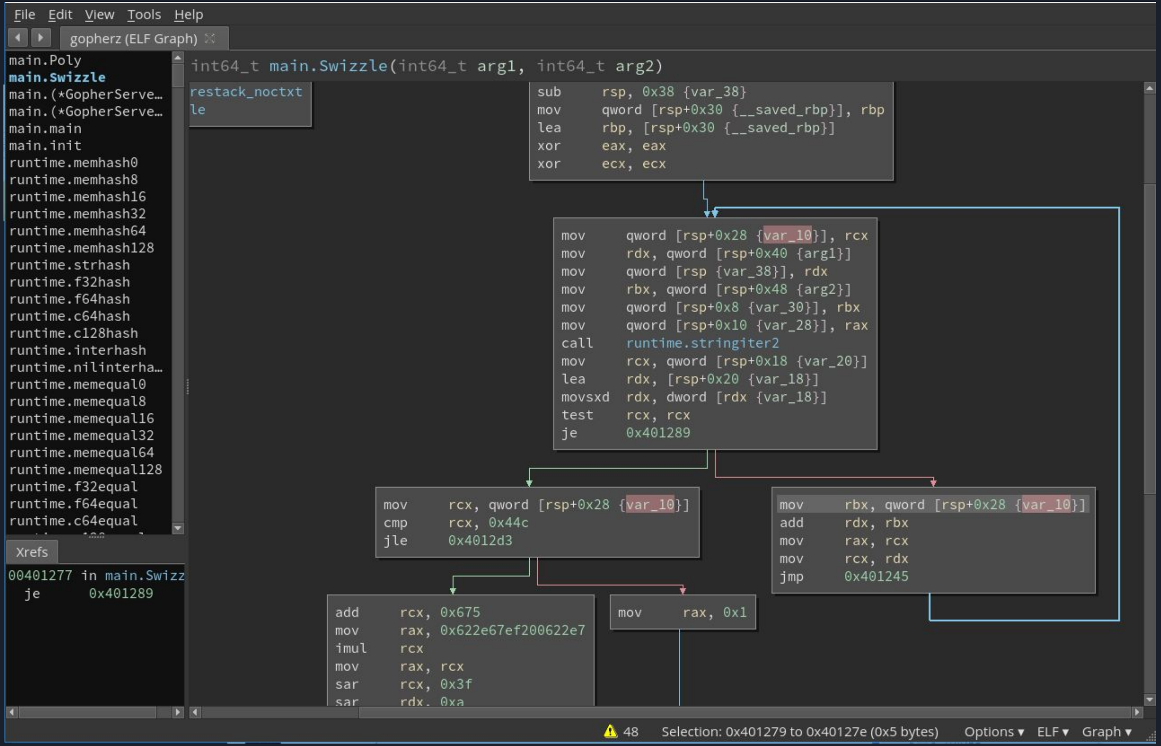


```
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
runtime.c128equal
```

```
00401906 in main.(*Gop
  jmp      main.(*Gophe
```

```
void* main.(*GopherServer).handleRequest(int64_t* arg1, uint64_t arg2)

mov     qword [rsp {var_120}], rcx
mov     qword [rsp+0x8], rax
lea     rdx, [rel 0x525064]  {"26683125: p=::/0==> @@@ AAAAAhom…"}
mov     qword [rsp+0x10], rdx  {0x525064, "26683125: p=::/0==> @@@ AAAAAhom…"  }
mov     qword [rsp+0x18 {var_108}], 0x4
call    runtime.eqstring
movzx   eax, byte [rsp+0x20 {var_100}]
test    al, al
je      0x4016db

mov     rax, qword [rsp+0x38 {var_e8}]
mov     rcx, qword [rsp+0x48 {var_d8}]
jmp     0x4015b0

mov     rax, 0x17
lea     rcx, [rel data_52858f]  {"icaterpillars grow\r\n.\r\ninter…"}
jmp     0x4015c8

cmp     rax, 0x57
je      0x401659

mov     qword [rsp {var_120}], rcx
mov     qword [rsp+0x8], rax
lea     rax, [rel 0x52cd6d]  {"457872149190039938449409450797725…"}
mov     qword [rsp+0x10], rax  {0x52cd6d, "457872149190039938449409450797725…"  }
mov     qword [rsp+0x18 {var_108}], 0x57
call    runtime.eqstring
movzx   eax, byte [rsp+0x20 {var_100}]
test    al, al
```

# Disassembly



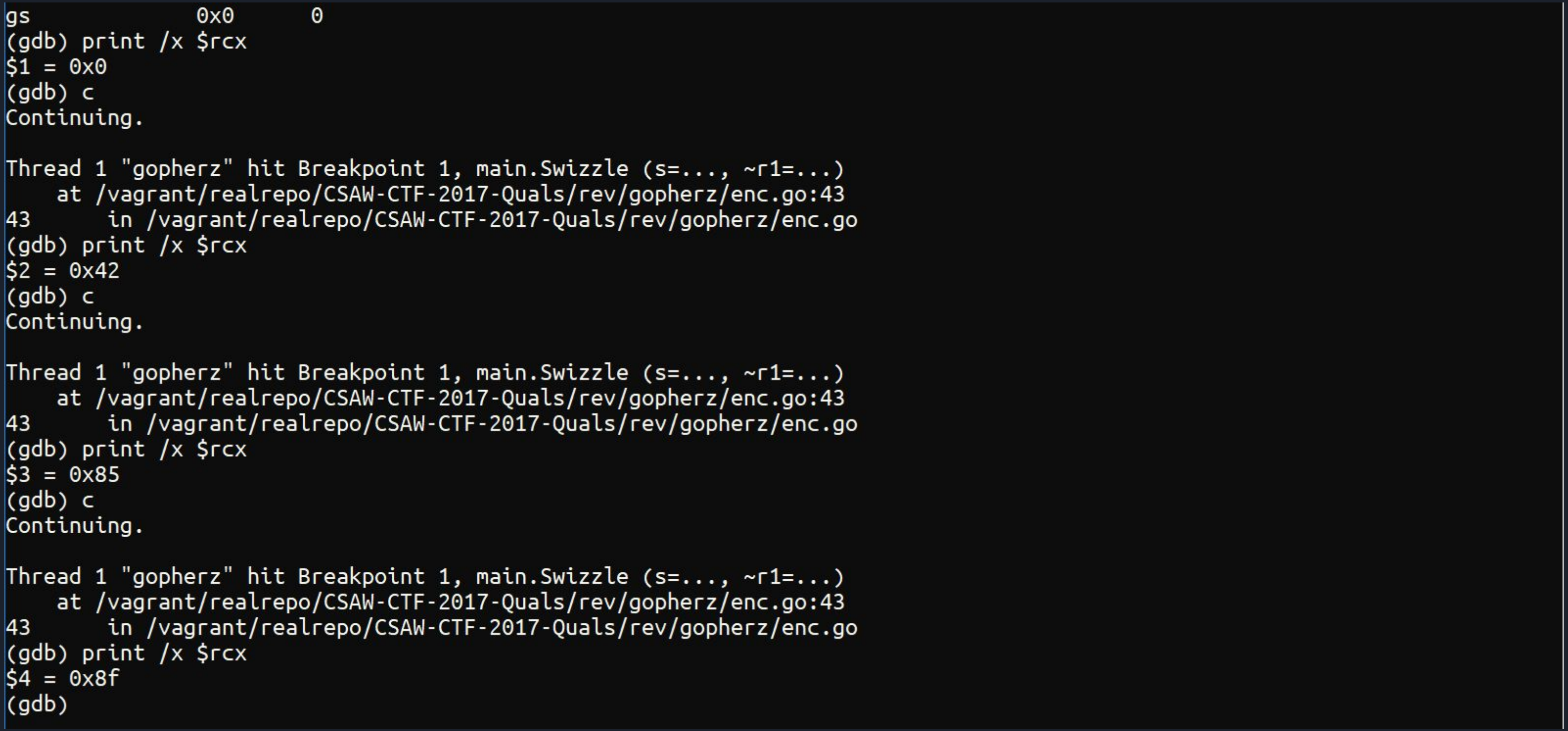
```
main.Poly
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
```

```
00401277 in main.Swizz
  je      0x401289
```

```
int64_t main.Swizzle(int64_t arg1, int64_t arg2)

restack_noctxt
le

sub     rsp, 0x38 {var_38}
mov     qword [rsp+0x30 {__saved_rbp}], rbp
lea     rbp, [rsp+0x30 {__saved_rbp}]
xor     eax, eax
xor     ecx, ecx

mov     qword [rsp+0x28 {var_10}], rcx
mov     rdx, qword [rsp+0x40 {arg1}]
mov     qword [rsp {var_38}], rdx
mov     rbx, qword [rsp+0x48 {arg2}]
mov     qword [rsp+0x8 {var_30}], rbx
mov     qword [rsp+0x10 {var_28}], rax
call    runtime.stringiter2
mov     rcx, qword [rsp+0x18 {var_20}]
lea     rdx, [rsp+0x20 {var_18}]
movsxd  rdx, dword [rdx {var_18}]
test    rcx, rcx
je      0x401289

mov     rcx, qword [rsp+0x28 {var_10}]
cmp     rcx, 0x44c
jle     0x4012d3

mov     rbx, qword [rsp+0x28 {var_10}]
add     rdx, rbx
mov     rax, rcx
mov     rcx, rdx
jmp     0x401245

add     rcx, 0x675
mov     rax, 0x622e67ef200622e7
imul    rcx
mov     rax, rcx
sar     rcx, 0x3f
sar     rdx, 0xa

mov     rax, 0x1
```

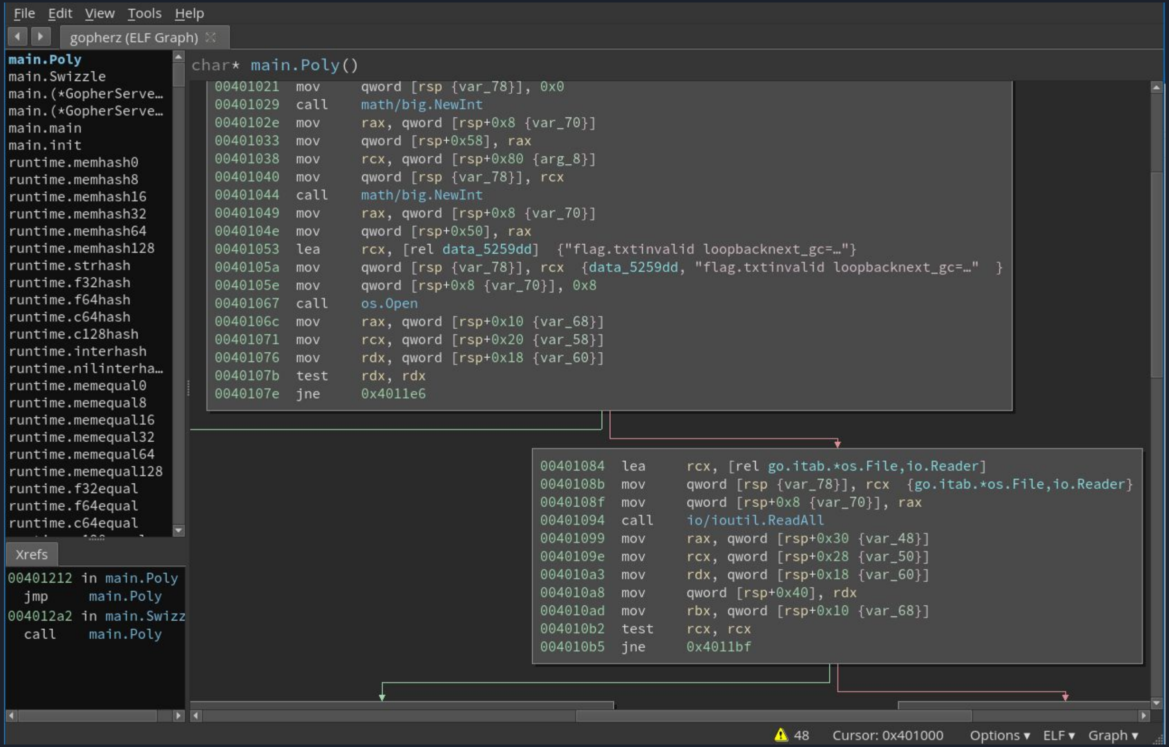
⚠ 48    Selection: 0x401279 to 0x40127e (0x5 bytes)

# Disassembly



```
gs             0x0      0
(gdb) print /x $rcx
$1 = 0x0
(gdb) c
Continuing.

Thread 1 "gopherz" hit Breakpoint 1, main.Swizzle (s=..., ~r1=...)
    at /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go:43
43      in /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go
(gdb) print /x $rcx
$2 = 0x42
(gdb) c
Continuing.

Thread 1 "gopherz" hit Breakpoint 1, main.Swizzle (s=..., ~r1=...)
    at /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go:43
43      in /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go
(gdb) print /x $rcx
$3 = 0x85
(gdb) c
Continuing.

Thread 1 "gopherz" hit Breakpoint 1, main.Swizzle (s=..., ~r1=...)
    at /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go:43
43      in /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go
(gdb) print /x $rcx
$4 = 0x8f
(gdb)
```

# Disassembly



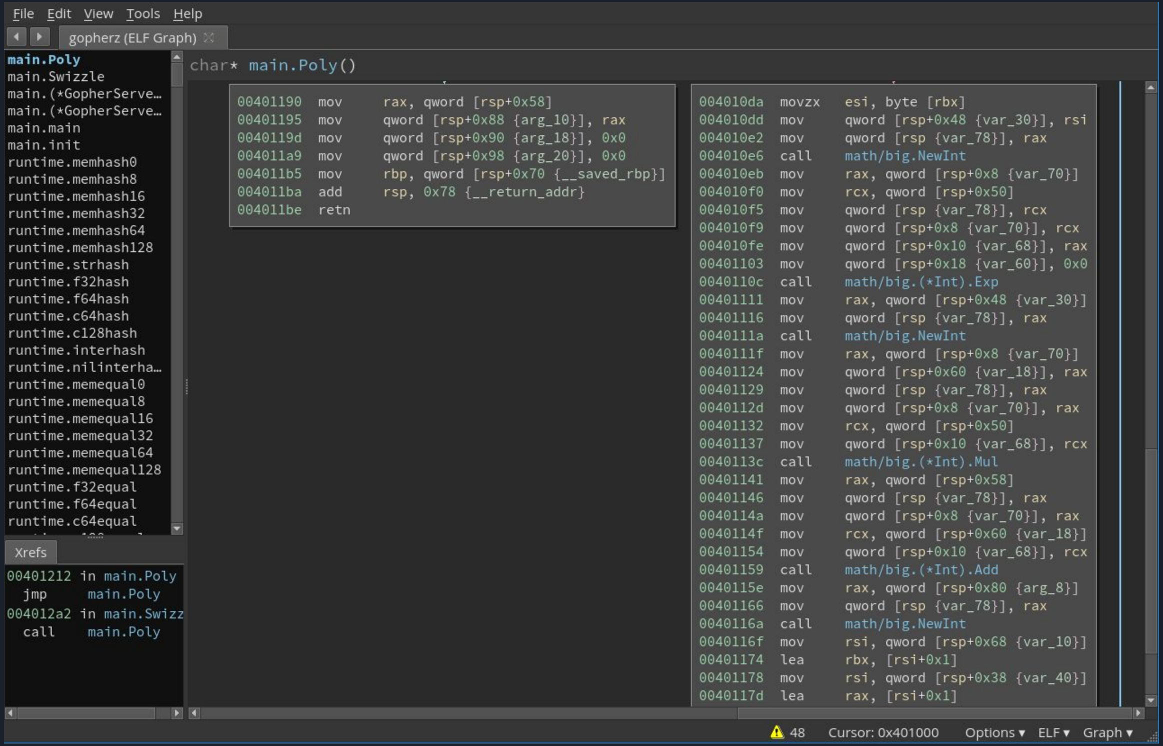
```
main.Poly
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
```

Xrefs

```
004011212 in main.Poly
  jmp      main.Poly
004012a2 in main.Swizz
  call     main.Poly
```

```
char* main.Poly()
00401021  mov     qword [rsp {var_78}], 0x0
00401029  call    math/big.NewInt
0040102e  mov     rax, qword [rsp+0x8 {var_70}]
00401033  mov     qword [rsp+0x58], rax
00401038  mov     rcx, qword [rsp+0x80 {arg_8}]
00401040  mov     qword [rsp {var_78}], rcx
00401044  call    math/big.NewInt
00401049  mov     rax, qword [rsp+0x8 {var_70}]
0040104e  mov     qword [rsp+0x50], rax
00401053  lea     rcx, [rel data_5259dd]  {"flag.txtinvalid loopbacknext_gc=…"}
0040105a  mov     qword [rsp {var_78}], rcx  {data_5259dd, "flag.txtinvalid loopbacknext_gc=…"  }
0040105e  mov     qword [rsp+0x8 {var_70}], 0x8
00401067  call    os.Open
0040106c  mov     rax, qword [rsp+0x10 {var_68}]
00401071  mov     rcx, qword [rsp+0x20 {var_58}]
00401076  mov     rdx, qword [rsp+0x18 {var_60}]
0040107b  test    rdx, rdx
0040107e  jne     0x4011e6

00401084  lea     rcx, [rel go.itab.*os.File,io.Reader]
0040108b  mov     qword [rsp {var_78}], rcx  {go.itab.*os.File,io.Reader}
0040108f  mov     qword [rsp+0x8 {var_70}], rax
00401094  call    io/ioutil.ReadAll
00401099  mov     rax, qword [rsp+0x30 {var_48}]
0040109e  mov     rcx, qword [rsp+0x28 {var_50}]
004010a3  mov     rdx, qword [rsp+0x18 {var_60}]
004010a8  mov     qword [rsp+0x40], rdx
004010ad  mov     rbx, qword [rsp+0x10 {var_68}]
004010b2  test    rcx, rcx
004010b5  jne     0x4011bf
```

# Disassembly



```
main.Poly
main.Swizzle
main.(*GopherServe…
main.(*GopherServe…
main.main
main.init
runtime.memhash0
runtime.memhash8
runtime.memhash16
runtime.memhash32
runtime.memhash64
runtime.memhash128
runtime.strhash
runtime.f32hash
runtime.f64hash
runtime.c64hash
runtime.c128hash
runtime.interhash
runtime.nilinterha…
runtime.memequal0
runtime.memequal8
runtime.memequal16
runtime.memequal32
runtime.memequal64
runtime.memequal128
runtime.f32equal
runtime.f64equal
runtime.c64equal
```

```
00401212 in main.Poly
  jmp     main.Poly
004012a2 in main.Swizz
  call    main.Poly
```

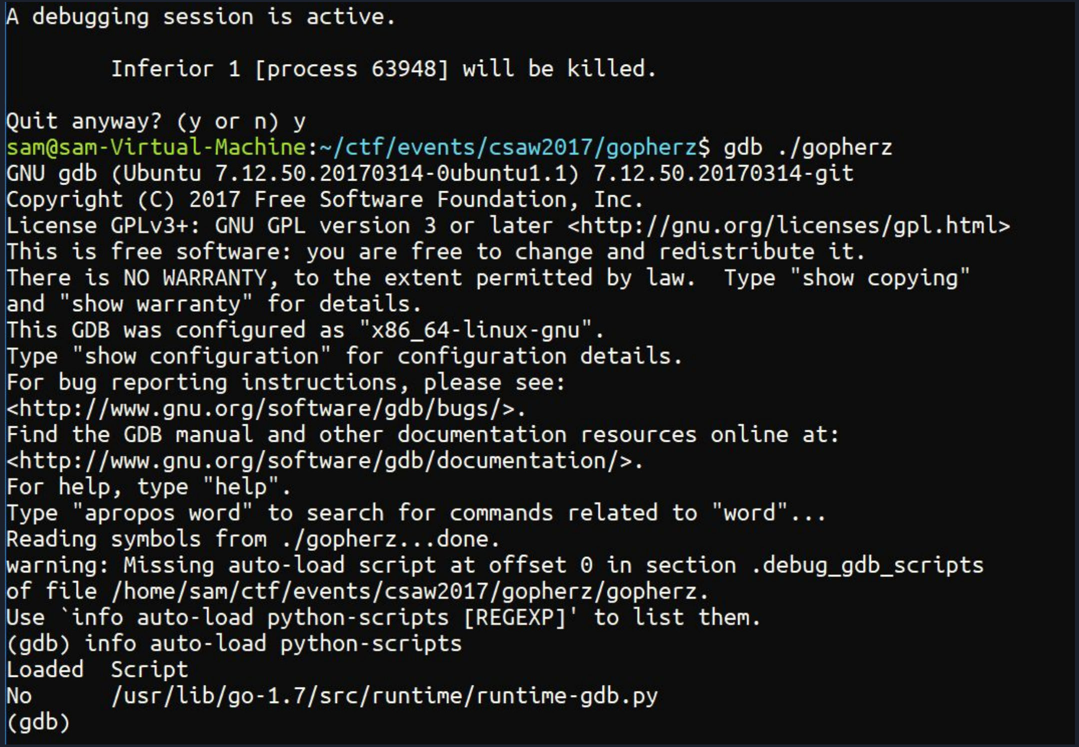
```
char* main.Poly()
```

```
00401190  mov     rax, qword [rsp+0x58]
00401195  mov     qword [rsp+0x88 {arg_10}], rax
0040119d  mov     qword [rsp+0x90 {arg_18}], 0x0
004011a9  mov     qword [rsp+0x98 {arg_20}], 0x0
004011b5  mov     rbp, qword [rsp+0x70 {__saved_rbp}]
004011ba  add     rsp, 0x78 {__return_addr}
004011be  retn
```

```
004010da  movzx   esi, byte [rbx]
004010dd  mov     qword [rsp+0x48 {var_30}], rsi
004010e2  mov     qword [rsp {var_78}], rax
004010e6  call    math/big.NewInt
004010eb  mov     rax, qword [rsp+0x8 {var_70}]
004010f0  mov     rcx, qword [rsp+0x50]
004010f5  mov     qword [rsp {var_78}], rcx
004010f9  mov     qword [rsp+0x8 {var_70}], rcx
004010fe  mov     qword [rsp+0x10 {var_68}], rax
00401103  mov     qword [rsp+0x18 {var_60}], 0x0
0040110c  call    math/big.(*Int).Exp
00401111  mov     rax, qword [rsp+0x48 {var_30}]
00401116  mov     qword [rsp {var_78}], rax
0040111a  call    math/big.NewInt
0040111f  mov     rax, qword [rsp+0x8 {var_70}]
00401124  mov     qword [rsp+0x60 {var_18}], rax
00401129  mov     qword [rsp {var_78}], rax
0040112d  mov     qword [rsp+0x8 {var_70}], rax
00401132  mov     rcx, qword [rsp+0x50]
00401137  mov     qword [rsp+0x10 {var_68}], rcx
0040113c  call    math/big.(*Int).Mul
00401141  mov     rax, qword [rsp+0x58]
00401146  mov     qword [rsp {var_78}], rax
0040114a  mov     qword [rsp+0x8 {var_70}], rax
0040114f  mov     rcx, qword [rsp+0x60 {var_18}]
00401154  mov     qword [rsp+0x10 {var_68}], rcx
00401159  call    math/big.(*Int).Add
0040115e  mov     rax, qword [rsp+0x80 {arg_8}]
00401166  mov     qword [rsp {var_78}], rax
0040116a  call    math/big.NewInt
0040116f  mov     rsi, qword [rsp+0x68 {var_10}]
00401174  lea     rbx, [rsi+0x1]
00401178  mov     rsi, qword [rsp+0x38 {var_40}]
0040117d  lea     rax, [rsi+0x1]
```

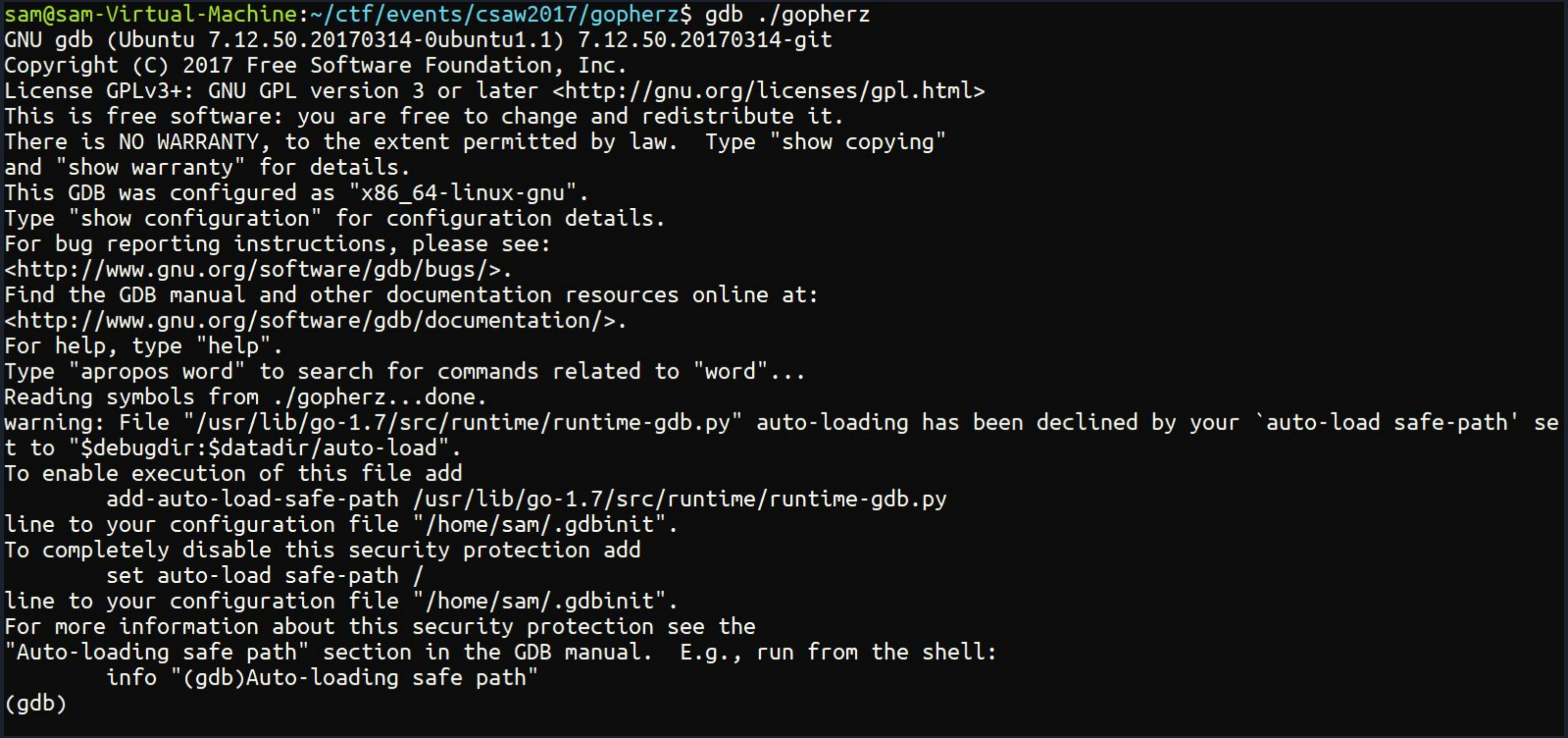
⚠ 48    Cursor: 0x401000

# Disassembly



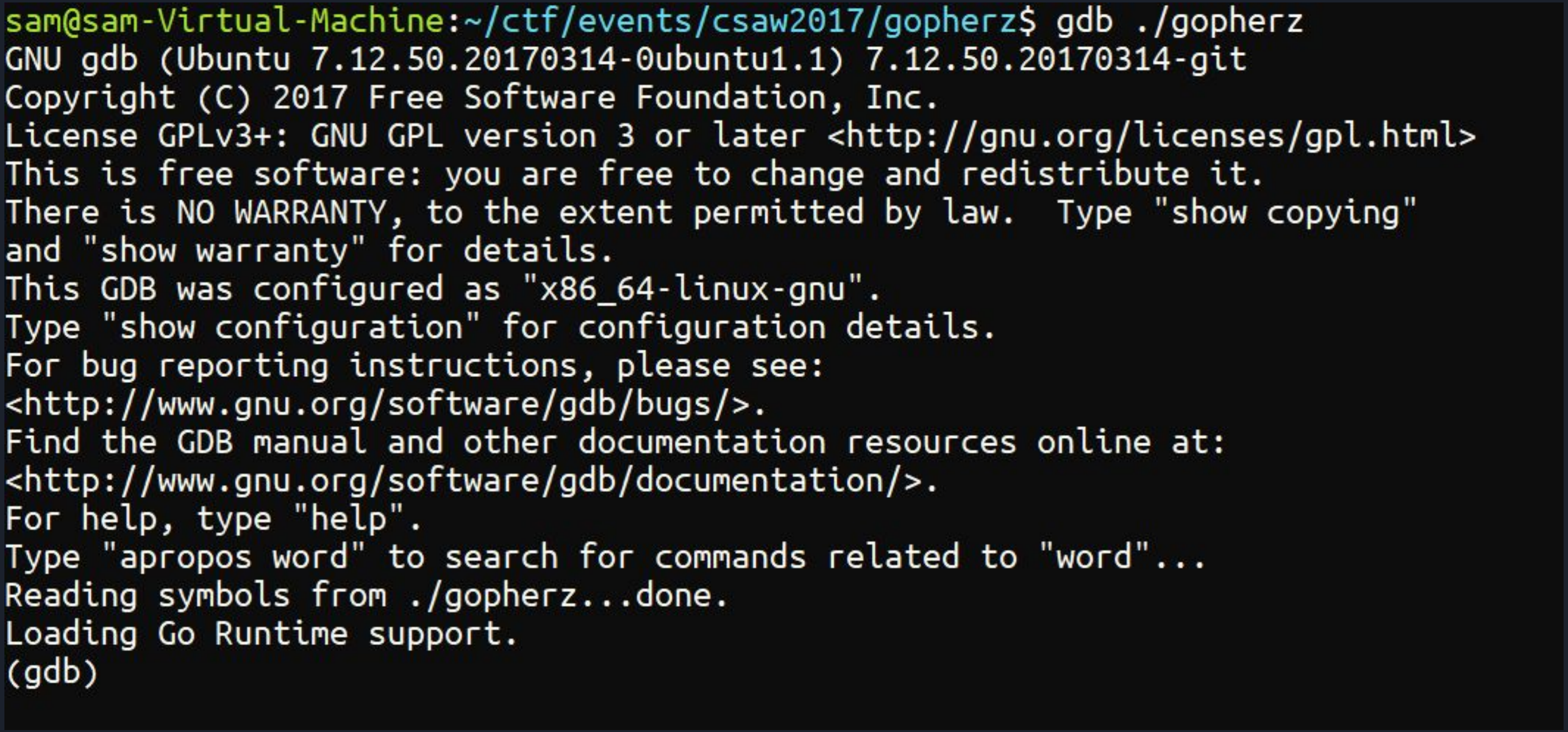
```
A debugging session is active.

        Inferior 1 [process 63948] will be killed.

Quit anyway? (y or n) y
sam@sam-Virtual-Machine:~/ctf/events/csaw2017/gopherz$ gdb ./gopherz
GNU gdb (Ubuntu 7.12.50.20170314-0ubuntu1.1) 7.12.50.20170314-git
Copyright (C) 2017 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./gopherz...done.
warning: Missing auto-load script at offset 0 in section .debug_gdb_scripts
of file /home/sam/ctf/events/csaw2017/gopherz/gopherz.
Use `info auto-load python-scripts [REGEXP]' to list them.
(gdb) info auto-load python-scripts
Loaded  Script
No      /usr/lib/go-1.7/src/runtime/runtime-gdb.py
(gdb)
```

# Disassembly



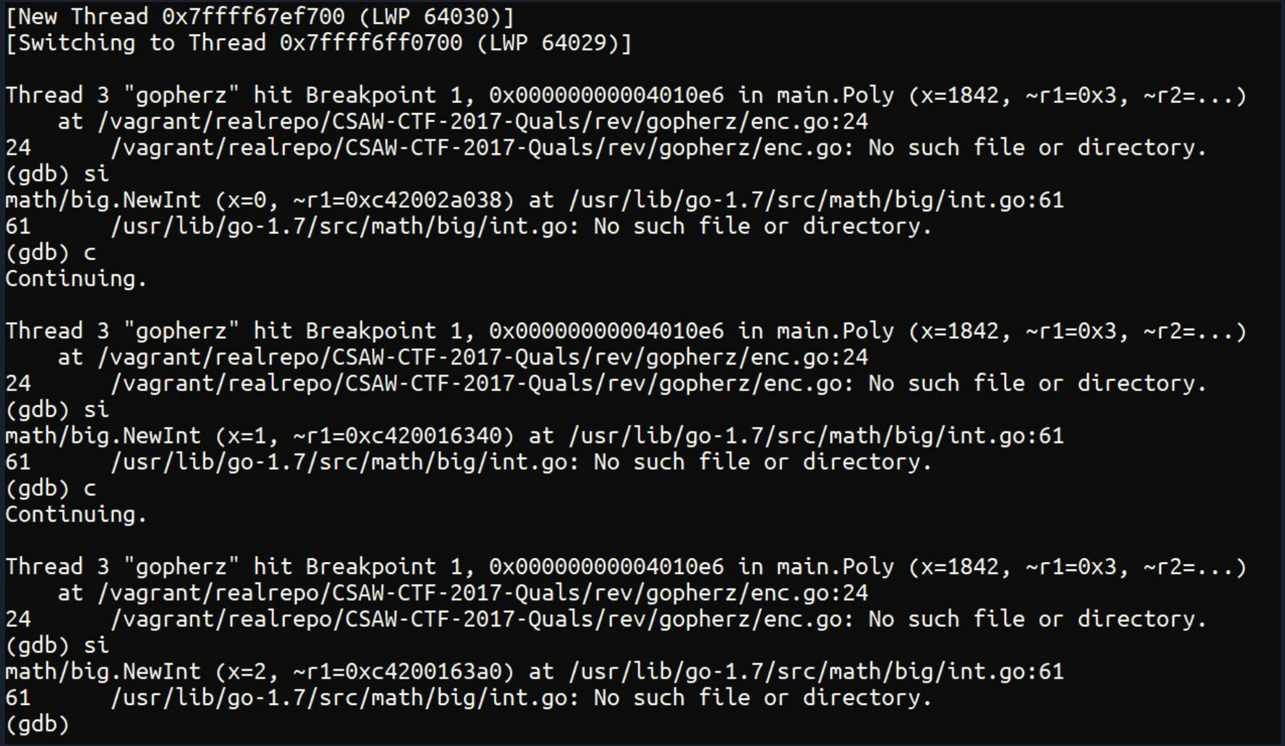
```
sam@sam-Virtual-Machine:~/ctf/events/csaw2017/gopherz$ gdb ./gopherz
GNU gdb (Ubuntu 7.12.50.20170314-0ubuntu1.1) 7.12.50.20170314-git
Copyright (C) 2017 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./gopherz...done.
warning: File "/usr/lib/go-1.7/src/runtime/runtime-gdb.py" auto-loading has been declined by your `auto-load safe-path' se
t to "$debugdir:$datadir/auto-load".
To enable execution of this file add
        add-auto-load-safe-path /usr/lib/go-1.7/src/runtime/runtime-gdb.py
line to your configuration file "/home/sam/.gdbinit".
To completely disable this security protection add
        set auto-load safe-path /
line to your configuration file "/home/sam/.gdbinit".
For more information about this security protection see the
"Auto-loading safe path" section in the GDB manual.  E.g., run from the shell:
        info "(gdb)Auto-loading safe path"
(gdb)
```

# Disassembly



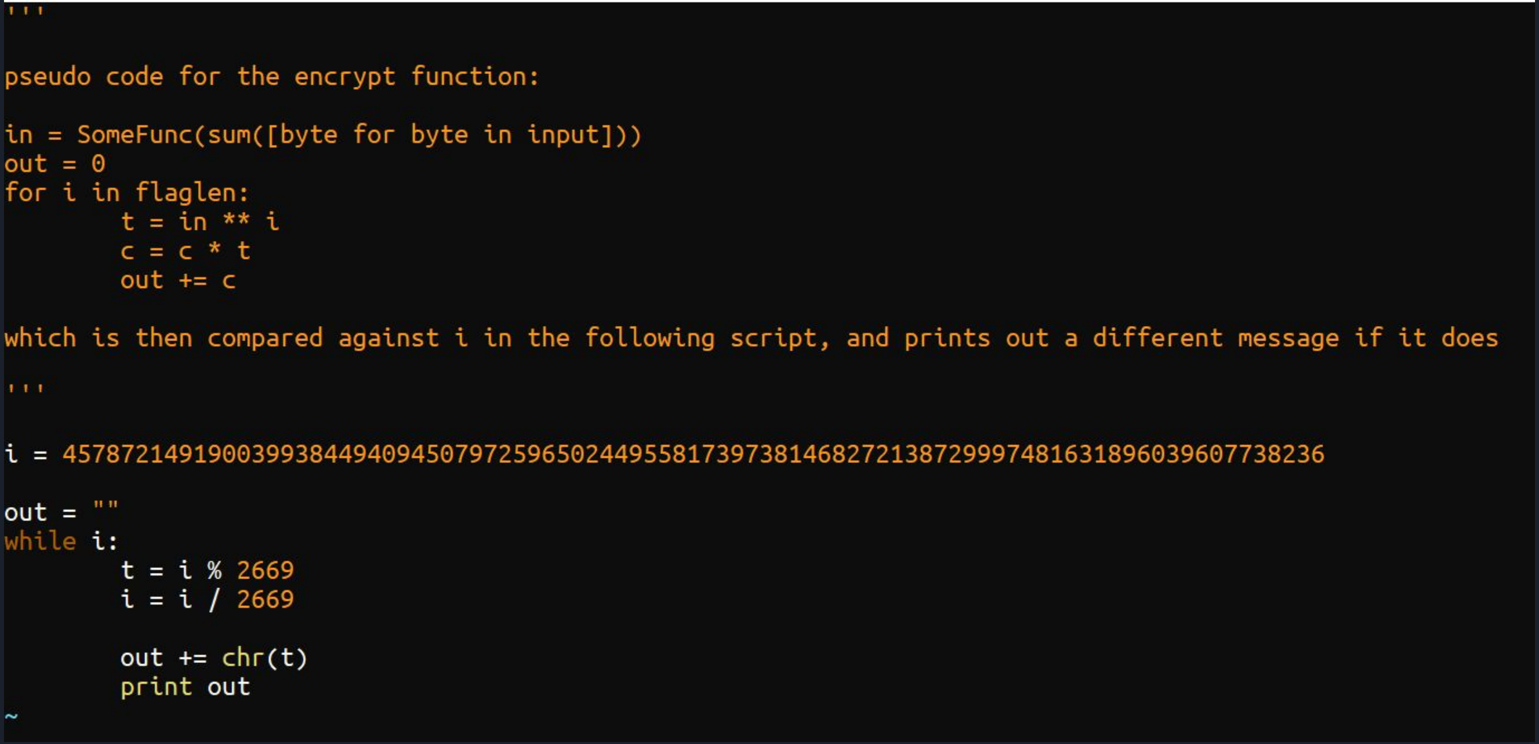
```
sam@sam-Virtual-Machine:~/ctf/events/csaw2017/gopherz$ gdb ./gopherz
GNU gdb (Ubuntu 7.12.50.20170314-0ubuntu1.1) 7.12.50.20170314-git
Copyright (C) 2017 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./gopherz...done.
Loading Go Runtime support.
(gdb)
```

# Disassembly



```
[New Thread 0x7ffff67ef700 (LWP 64030)]
[Switching to Thread 0x7ffff6ff0700 (LWP 64029)]

Thread 3 "gopherz" hit Breakpoint 1, 0x00000000004010e6 in main.Poly (x=1842, ~r1=0x3, ~r2=...)
    at /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go:24
24      /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go: No such file or directory.
(gdb) si
math/big.NewInt (x=0, ~r1=0xc42002a038) at /usr/lib/go-1.7/src/math/big/int.go:61
61      /usr/lib/go-1.7/src/math/big/int.go: No such file or directory.
(gdb) c
Continuing.

Thread 3 "gopherz" hit Breakpoint 1, 0x00000000004010e6 in main.Poly (x=1842, ~r1=0x3, ~r2=...)
    at /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go:24
24      /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go: No such file or directory.
(gdb) si
math/big.NewInt (x=1, ~r1=0xc420016340) at /usr/lib/go-1.7/src/math/big/int.go:61
61      /usr/lib/go-1.7/src/math/big/int.go: No such file or directory.
(gdb) c
Continuing.

Thread 3 "gopherz" hit Breakpoint 1, 0x00000000004010e6 in main.Poly (x=1842, ~r1=0x3, ~r2=...)
    at /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go:24
24      /vagrant/realrepo/CSAW-CTF-2017-Quals/rev/gopherz/enc.go: No such file or directory.
(gdb) si
math/big.NewInt (x=2, ~r1=0xc4200163a0) at /usr/lib/go-1.7/src/math/big/int.go:61
61      /usr/lib/go-1.7/src/math/big/int.go: No such file or directory.
(gdb)
```

# Disassembly



```
'''

pseudo code for the encrypt function:

in = SomeFunc(sum([byte for byte in input]))
out = 0
for i in flaglen:
        t = in ** i
        c = c * t
        out += c

which is then compared against i in the following script, and prints out a different message if it does

'''

i = 457872149190039938449409450797259650244955817397381468272138729997481631896039607738236

out = ""
while i:
        t = i % 2669
        i = i / 2669

        out += chr(t)
        print out
~
```

# More about me - Kudu Dynamics

- My Current Employer
- ~25 Engineers out in Chantilly VA
- Decades of experience building offensive and defensive cyber security solutions
- Current openings include junior engineers (and senior roles, too)
- Employed 3 interns Summer 2017, expect similar Summer 2018
- Interesting work, fun environment, great benefits, etc.

# Kudu Interns

- Paid Internship
- Housing Allowance
- Mentorship opportunities with senior engineers, direct access to real program work, no busy work
- Kudu does a great job of teaching junior engineers
- Cross program work opportunities (ex: Andy working on SC2 then getting to work on PP)
- Interns get really cool, great equipment to work on as well as an intern only office to work directly with
- your peers
- Fun actives during the summer, last year we went to an escape room and had an eclipse viewing party
- VR, 3D printer, scooters, go carts, snacks and fun

# Kudu Intern Interview

- You will be assigned a paid program, this program typically takes a week or 2 to complete, the program is assigned based on your areas of interest and experience. Each program has been selected based off real problems we are solving. The program gives you a chance to become familiar with the work we do and see if you like it and also gives us the opportunity to gauge your technical skills.
- Once the program is complete you will present it to our team as your interview. Regardless if you gethired or not you will be paid.
- Our summer internships are flexible but typically start in May and end in Aug
- We do allow Co-ops (work much like internships, but can be anytime during the year based off school schedule
- Part-time hires will not require a project, but there will be a formal interview process