Debugging without Code

Random Tips on How to Debug Closed Source

הקדמת הרב המחבר

אמר המחבר החיבור הזה לא חברתיו ללמד לבני האדם את אשר לא ידעו אלא להזכירם את הידוע להם כבר ומפורסם אצלם פרסום גדול. כי לא תמצא ברוב דברי אלא דברים שרוב בני האדם יודעים אותם ולא מסתפקים בהם כלל. אלא שכפי רוב פרסומם וכנגד מה שאמתתם גלויה לכל כך ההעלם מהם מצוי מאד וההשכחה רבה. ע"כ אין התועלת הנלקט מזה הספר יוצא מן הקריאה בו פעם אחת. כי כבר אפשר שלא ימצא הקורא בשכלו חידושים אחר קריאתו שלא

Why?

ICE

Internal

Compiler

Error

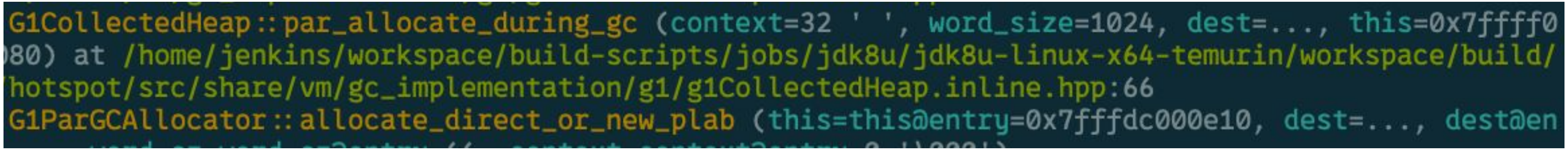
External Tools

Your UI toolkit shared object

Question At Hand

JVM crashed

What was the value of dest on crash



```
G1CollectedHeap::par_allocate_during_gc (context=32 ' ', word_size=1024, dest=..., this=0x7ffff0
)80) at /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/
'hotspot/src/share/vm/gc_implementation/g1/g1CollectedHeap.inline.hpp:66
G1ParGCAllocator::allocate_direct_or_new_plab (this=this@entry=0x7fffdc000e10, dest=..., dest@en
```

debuginfod

Based on buildid embeded in ELF

Available for Popular Linux Distro

Microsoft Public Symbol Server

Nightly Builds?

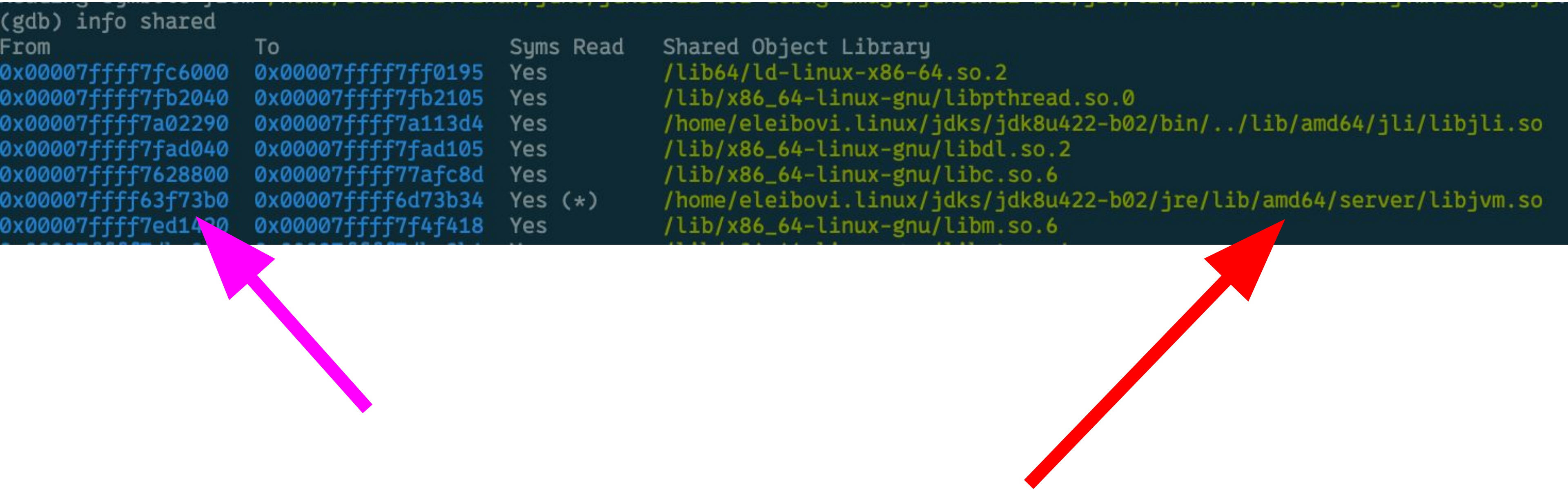
Those are usually for development

Might include debug symbols

First Problem Function Arguments

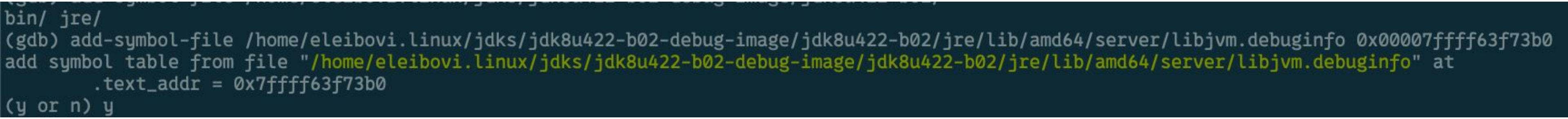
We need debug symbols for that!

info shared

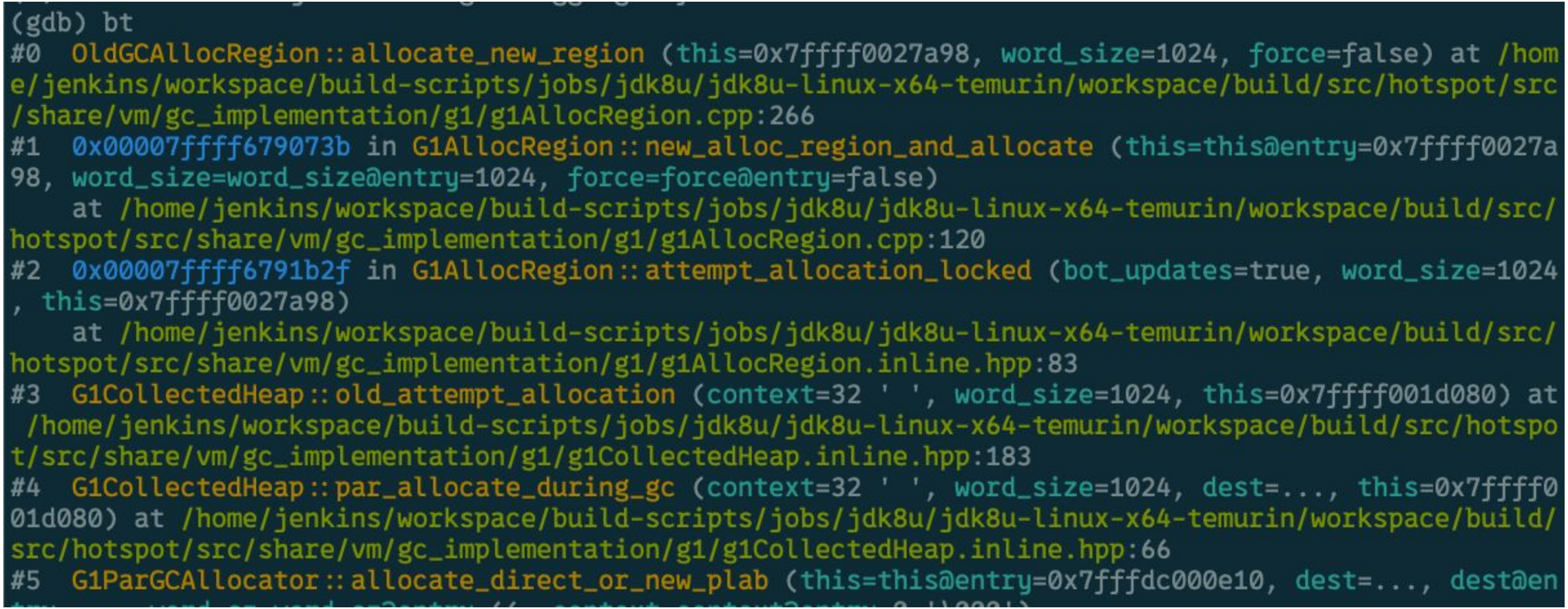


```
(gdb) info shared
From                To                  Syms Read   Shared Object Library
0x00007ffff7fc6000  0x00007ffff7ff0195  Yes         /lib64/ld-linux-x86-64.so.2
0x00007ffff7fb2040  0x00007ffff7fb2105  Yes         /lib/x86_64-linux-gnu/libpthread.so.0
0x00007ffff7a02290  0x00007ffff7a113d4  Yes         /home/eleibovi.linux/jdks/jdk8u422-b02/bin/../lib/amd64/jli/libjli.so
0x00007ffff7fad040  0x00007ffff7fad105  Yes         /lib/x86_64-linux-gnu/libdl.so.2
0x00007ffff7628800  0x00007ffff77afc8d  Yes         /lib/x86_64-linux-gnu/libc.so.6
0x00007ffff63f73b0  0x00007ffff6d73b34  Yes (*)     /home/eleibovi.linux/jdks/jdk8u422-b02/jre/lib/amd64/server/libjvm.so
0x00007ffff7ed1420  0x00007ffff7f4f418  Yes         /lib/x86_64-linux-gnu/libm.so.6
```

add-symbol-file

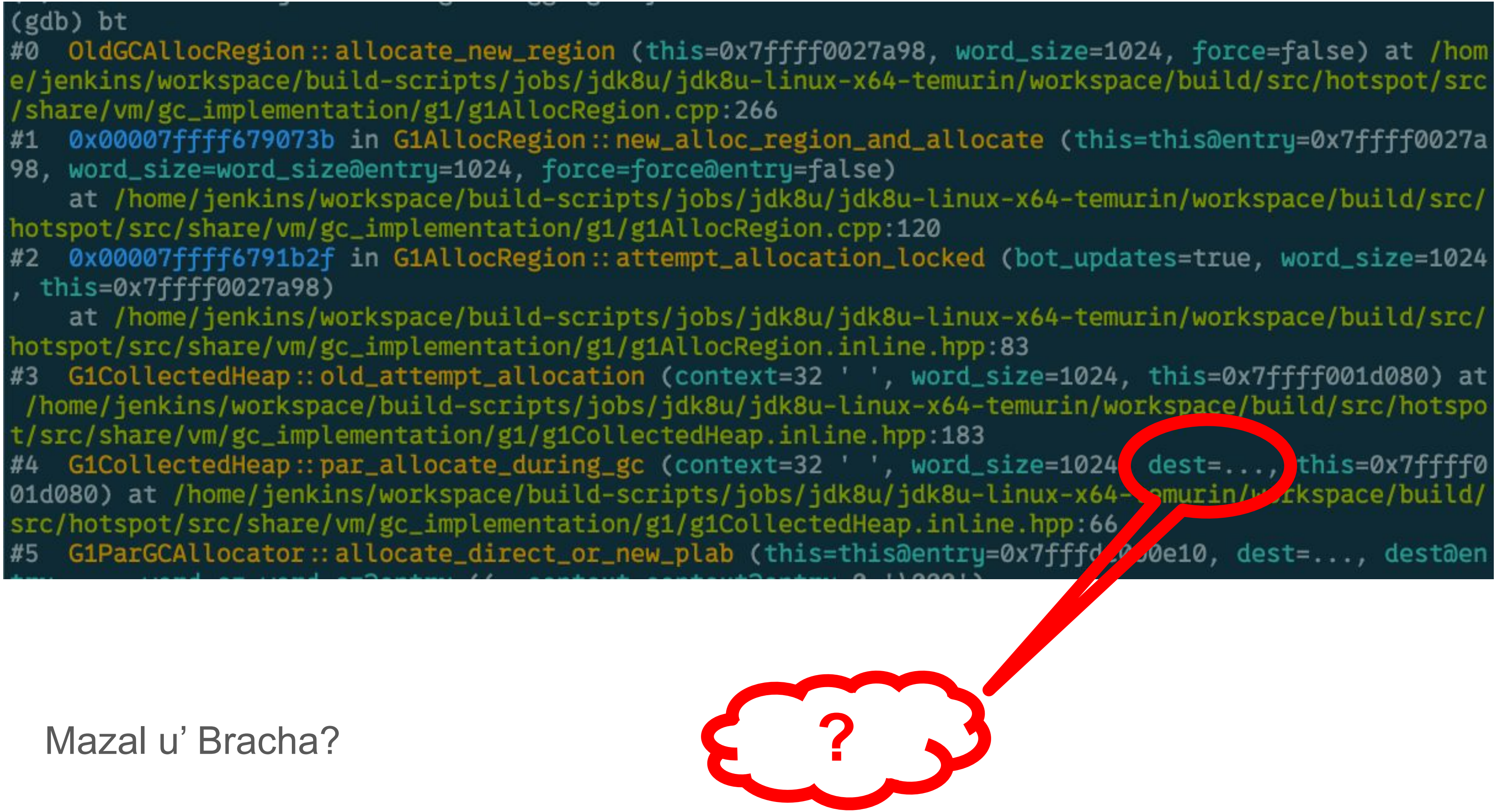


```
(gdb) add-symbol-file /home/eleibovi.linux/jdks/jdk8u422-b02-debug-image/jdk8u422-b02/
bin/ jre/
(gdb) add-symbol-file /home/eleibovi.linux/jdks/jdk8u422-b02-debug-image/jdk8u422-b02/jre/lib/amd64/server/libjvm.debuginfo 0x00007ffff63f73b0
add symbol table from file "/home/eleibovi.linux/jdks/jdk8u422-b02-debug-image/jdk8u422-b02/jre/lib/amd64/server/libjvm.debuginfo" at
        .text_addr = 0x7ffff63f73b0
(y or n) y
```



```
(gdb) bt
#0  OldGCAllocRegion::allocate_new_region (this=0x7ffff0027a98, word_size=1024, force=false) at /hom
e/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/hotspot/src
/share/vm/gc_implementation/g1/g1AllocRegion.cpp:266
#1  0x00007ffff679073b in G1AllocRegion::new_alloc_region_and_allocate (this=this@entry=0x7ffff0027a
98, word_size=word_size@entry=1024, force=force@entry=false)
    at /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/
hotspot/src/share/vm/gc_implementation/g1/g1AllocRegion.cpp:120
#2  0x00007ffff6791b2f in G1AllocRegion::attempt_allocation_locked (bot_updates=true, word_size=1024
, this=0x7ffff0027a98)
    at /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/
hotspot/src/share/vm/gc_implementation/g1/g1AllocRegion.inline.hpp:83
#3  G1CollectedHeap::old_attempt_allocation (context=32 ' ', word_size=1024, this=0x7ffff001d080) at
 /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/hotspo
t/src/share/vm/gc_implementation/g1/g1CollectedHeap.inline.hpp:183
#4  G1CollectedHeap::par_allocate_during_gc (context=32 ' ', word_size=1024, dest=..., this=0x7ffff0
01d080) at /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/
src/hotspot/src/share/vm/gc_implementation/g1/g1CollectedHeap.inline.hpp:66
#5  G1ParGCAllocator::allocate_direct_or_new_plab (this=this@entry=0x7fffdc000e10, dest=..., dest@en
```

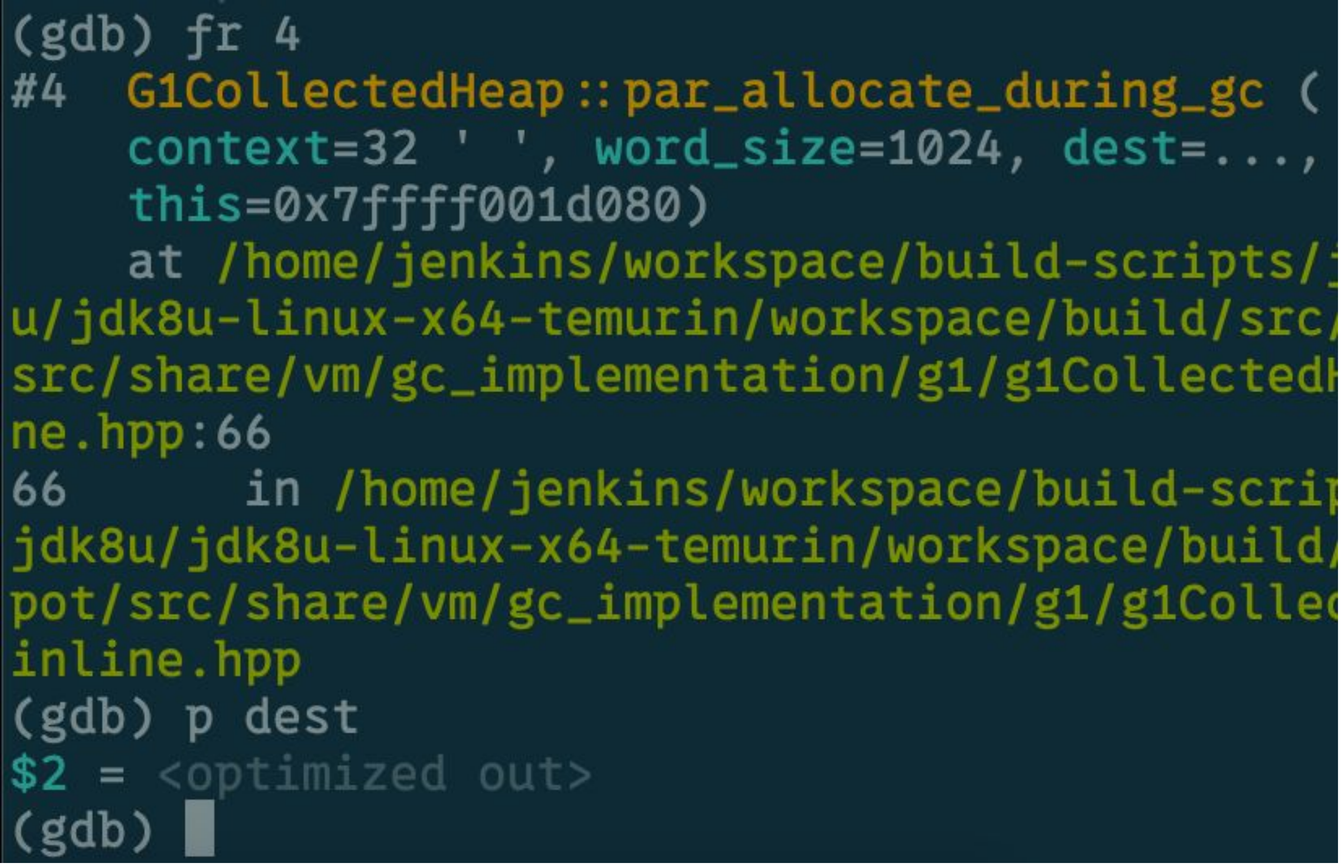
Mazal u’ Bracha



```
(gdb) bt
#0  OldGCAllocRegion::allocate_new_region (this=0x7ffff0027a98, word_size=1024, force=false) at /hom
e/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/hotspot/src
/share/vm/gc_implementation/g1/g1AllocRegion.cpp:266
#1  0x00007ffff679073b in G1AllocRegion::new_alloc_region_and_allocate (this=this@entry=0x7ffff0027a
98, word_size=word_size@entry=1024, force=force@entry=false)
    at /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/
hotspot/src/share/vm/gc_implementation/g1/g1AllocRegion.cpp:120
#2  0x00007ffff6791b2f in G1AllocRegion::attempt_allocation_locked (bot_updates=true, word_size=1024
, this=0x7ffff0027a98)
    at /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/
hotspot/src/share/vm/gc_implementation/g1/g1AllocRegion.inline.hpp:83
#3  G1CollectedHeap::old_attempt_allocation (context=32 ' ', word_size=1024, this=0x7ffff001d080) at
 /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/src/hotspo
t/src/share/vm/gc_implementation/g1/g1CollectedHeap.inline.hpp:183
#4  G1CollectedHeap::par_allocate_during_gc (context=32 ' ', word_size=1024, dest=..., this=0x7ffff0
01d080) at /home/jenkins/workspace/build-scripts/jobs/jdk8u/jdk8u-linux-x64-temurin/workspace/build/
src/hotspot/src/share/vm/gc_implementation/g1/g1CollectedHeap.inline.hpp:66
#5  G1ParGCAllocator::allocate_direct_or_new_plab (this=this@entry=0x7fffd0000e10, dest=..., dest@en
```

Mazal u’ Bracha?

Optimized Out. Now What?



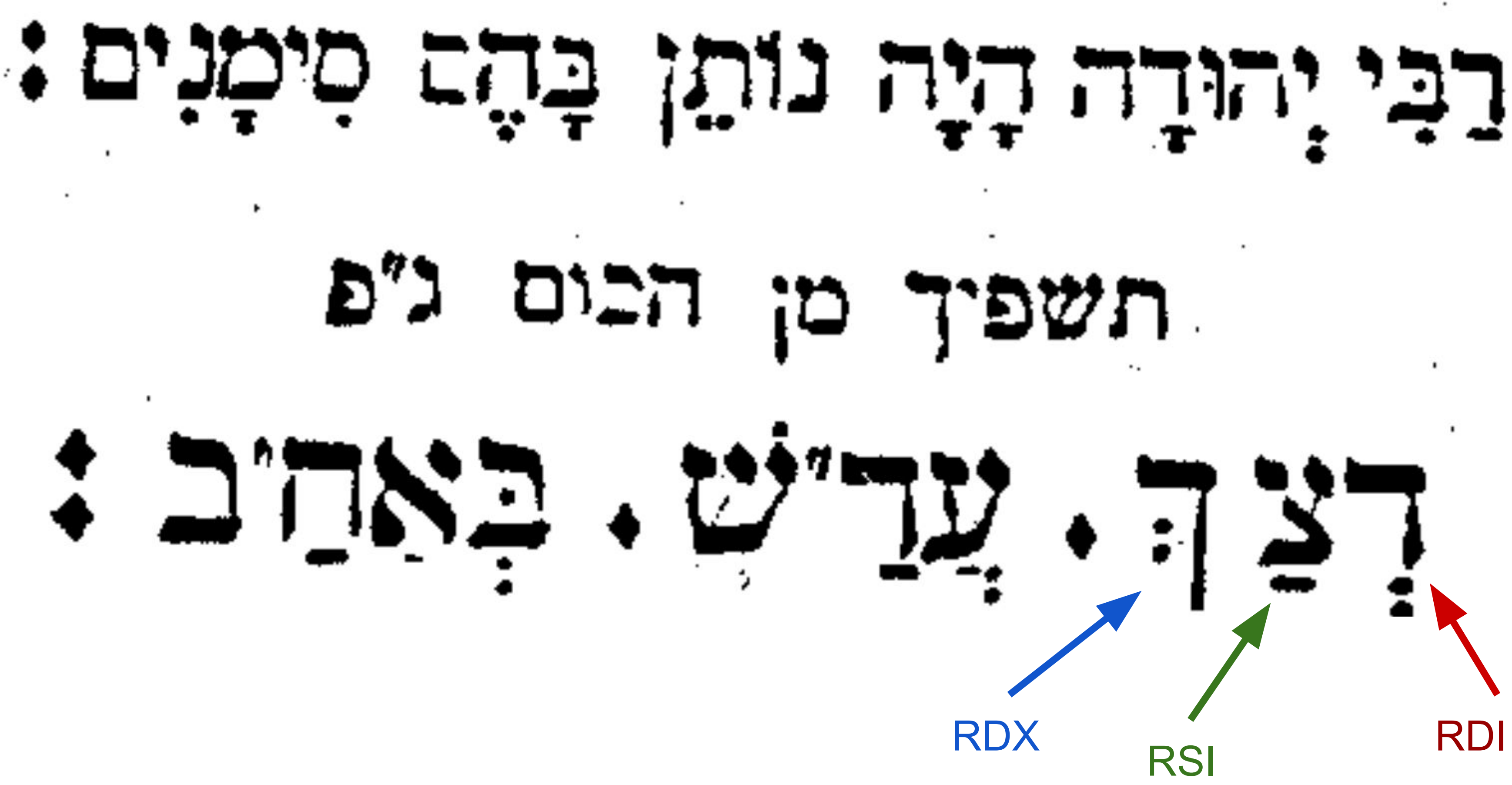
```
(gdb) fr 4
#4  G1CollectedHeap::par_allocate_during_gc (
    context=32 ' ', word_size=1024, dest=...,
    this=0x7ffff001d080)
    at /home/jenkins/workspace/build-scripts/j
u/jdk8u-linux-x64-temurin/workspace/build/src/
src/share/vm/gc_implementation/g1/g1CollectedH
ne.hpp:66
66          in /home/jenkins/workspace/build-scrip
jdk8u/jdk8u-linux-x64-temurin/workspace/build/
pot/src/share/vm/gc_implementation/g1/g1Collec
inline.hpp
(gdb) p dest
$2 = <optimized out>
(gdb) 
```

Optimized Out, now what?

Understanding Function Arguments

Calling Conventions

Never Lie



רַבִּי יְהוּדָה הָיָה נוֹתֵן בָּהֶם סִימָנִים׃

תשפך מן הכוס ג״פ

דְצַךְ. עֲדַ״שׁ. בְּאַחַ״ב׃

Break Higher on stack

There find out what *dest* was

gdb?

IF SOMETHING'S HARD TO DO, THEN IT'S NOT WORTH DOING.

gdb record

Didn’t work for me :(

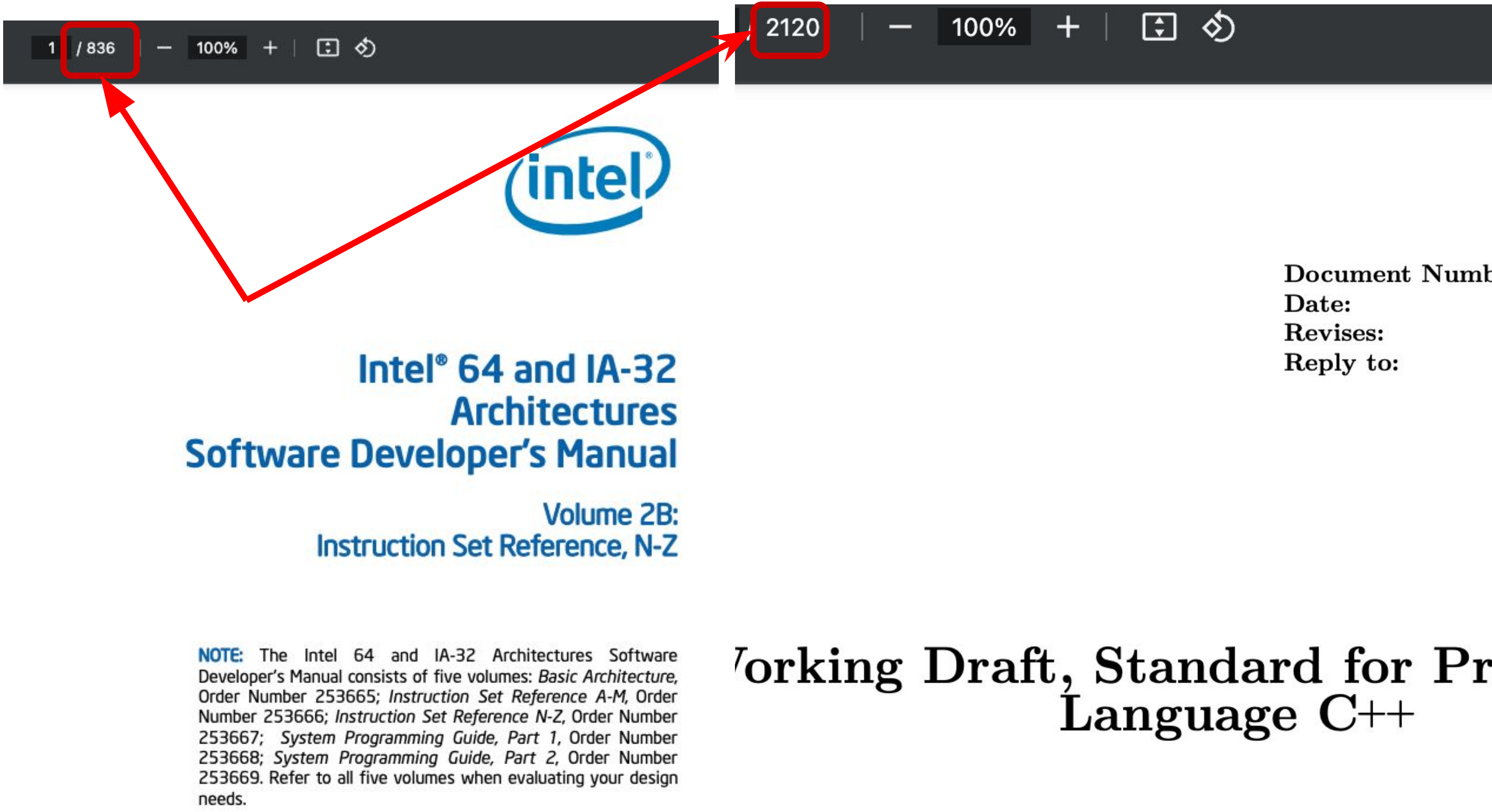
gdb trace?

You can't do that when your target is `multi-thread'

Breakpoint commands

Works, but slow

Decompilation?



Intel® 64 and IA-32 Architectures Software Developer's Manual

Volume 2B: Instruction Set Reference, N-Z

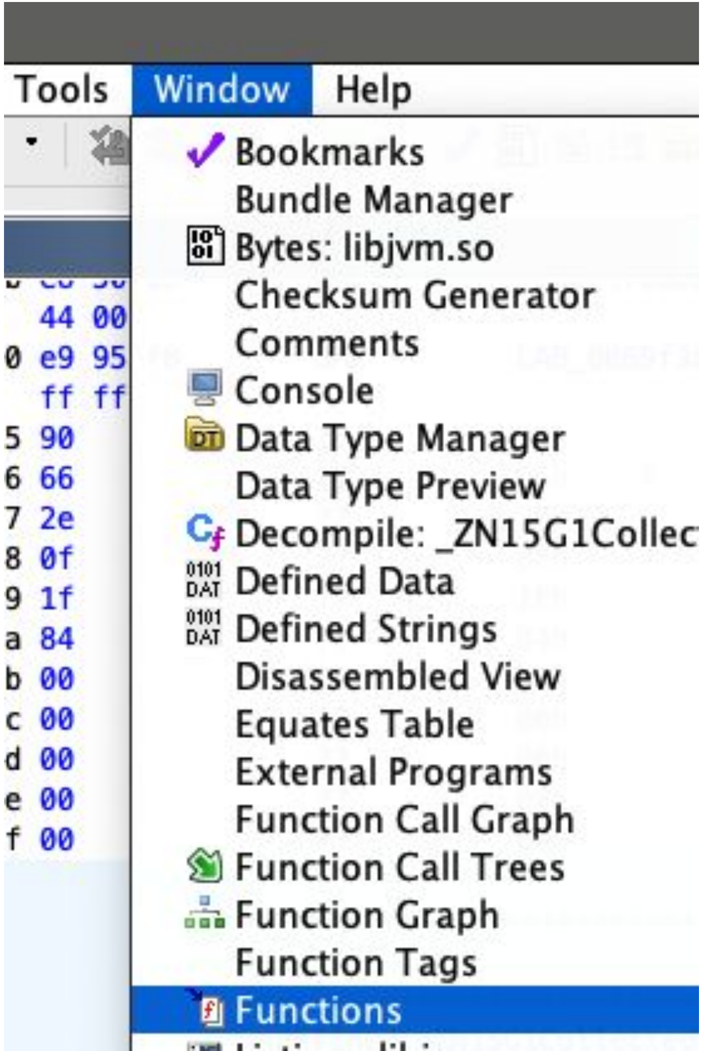
NOTE: The Intel 64 and IA-32 Architectures Software Developer's Manual consists of five volumes: *Basic Architecture*, Order Number 253665; *Instruction Set Reference A-M*, Order Number 253666; *Instruction Set Reference N-Z*, Order Number 253667; *System Programming Guide, Part 1*, Order Number 253668; *System Programming Guide, Part 2*, Order Number 253669. Refer to all five volumes when evaluating your design needs.

Document Numb
Date:
Revises:
Reply to:

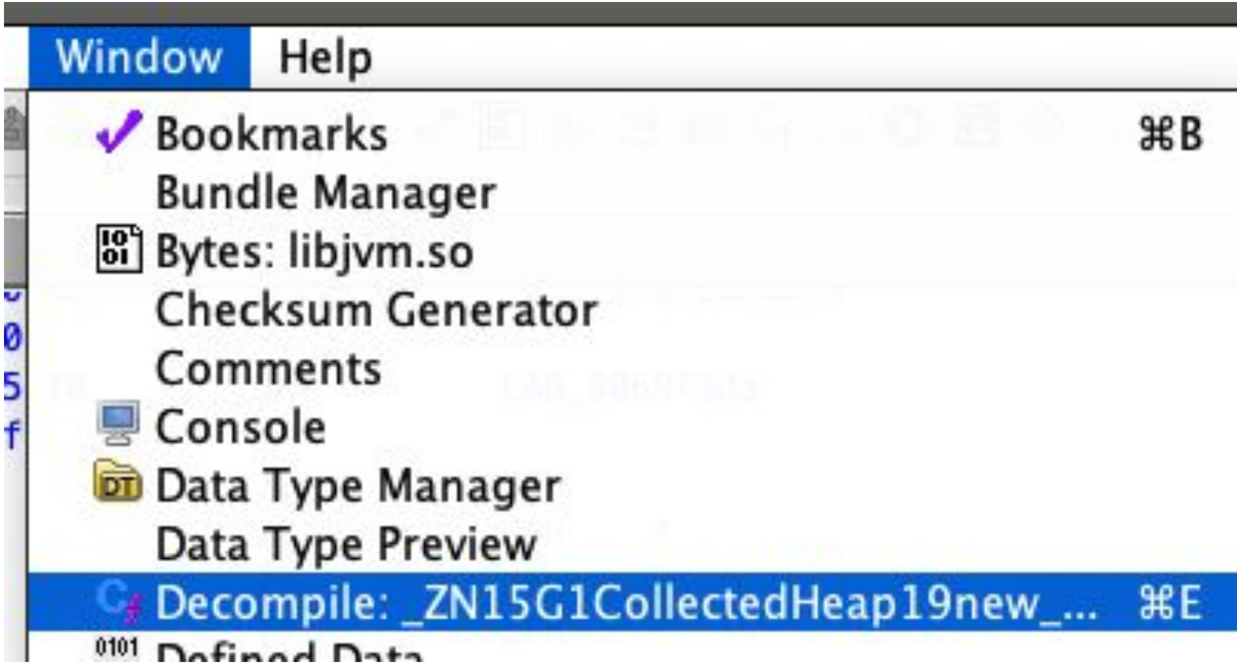
orking Draft, Standard for Pr Language C++

Search Function

Sometimes demangling fails

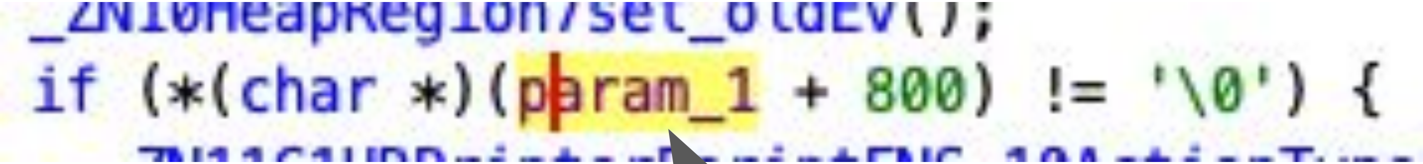


Decompile

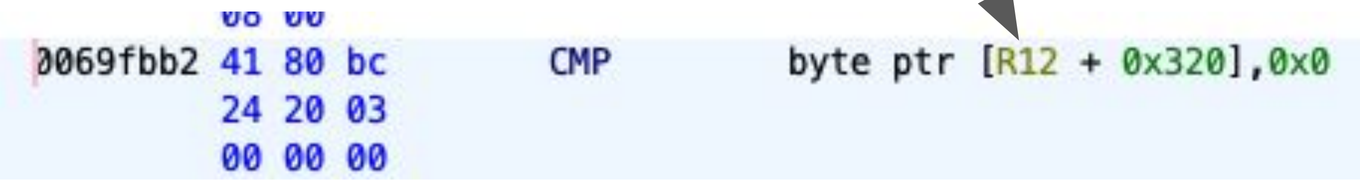

Window
Help
✓ Bookmarks ⌘B
Bundle Manager
Bytes: libjvm.so
Checksum Generator
Comments
Console
Data Type Manager
Data Type Preview
Decompile: _ZN15G1CollectedHeap19new_... ⌘E
Defined Data

Find Register

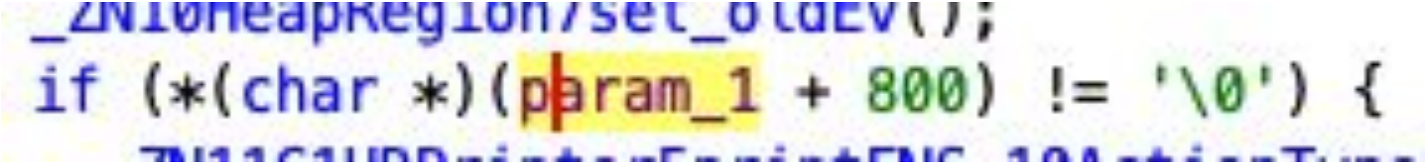
R12 contains first parameter to function



```
_ZN10HeapRegion7set_oldEv();
if (*(char *)(param_1 + 800) != '\0') {
```



```
                08 00
0069fbb2 41 80 bc         CMP         byte ptr [R12 + 0x320],0x0
         24 20 03
         00 00 00
```

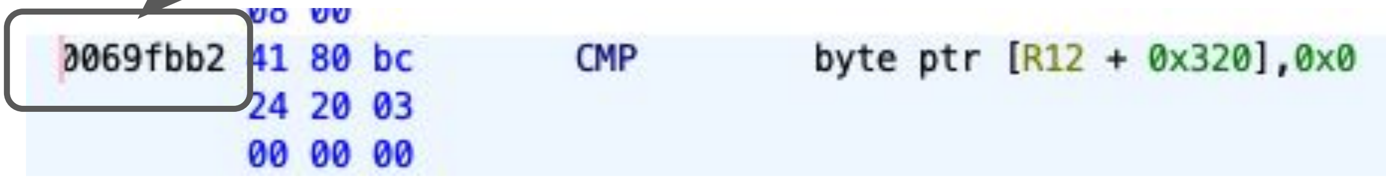


```
_ZN10HeapRegion7set_oldEv();
if (*(char *)(param_1 + 800) != '\0') {
```

Find Offset

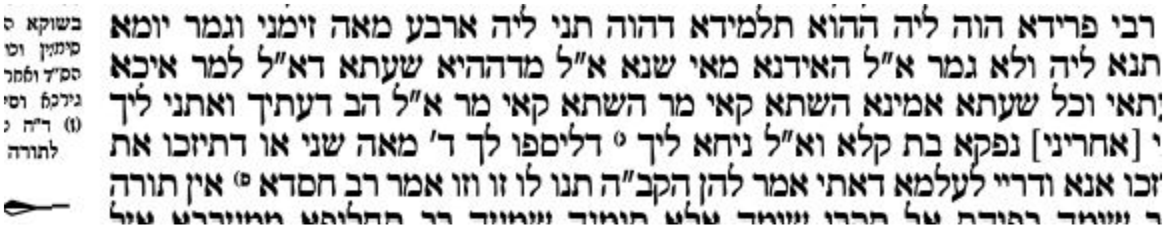
R12 contains first parameter to function

Breakpoint Here



```
          08 00
0069fbb2  41 80 bc        CMP        byte ptr [R12 + 0x320],0x0
          24 20 03
          00 00 00
```

Frida



בשוקא
סימנין וכו
הס"ד ומר
גילכא וסי
(1) ד"ה
לתורה

רבי פרידא הוה ליה ההוא תלמידא דהוה תני ליה ארבע מאה זימני וגמר יומא
תנא ליה ולא גמר א"ל האידנא מאי שנא א"ל מדההיא שעתא דא"ל למר איכא
יתאי וכל שעתא אמינא השתא קאי מר א"ל הב דעתיך ואתני ליך
י [אחריני] נפקא בת קלא וא"ל ניחא ליך ° דליספו לך ד' מאה שני או דתיזכו את
זכו אנא ודריי לעלמא דאתי אמר להן הקב"ה תנו לו זו וזו אמר רב חסדא ° אין תורה

Load Module

```
let m = Module.load("./libjvm.so");
```

Find Function

```
HeapRegion*OldGCAllocRegion::allocate_new_region(size_t word_size,
                                                 bool force) {
  assert(!force, "not supported for GC alloc regions");
  return _g1h->new_gc_alloc_region(word_size, count(),
                                   InCSetState::Old);
}
```

Find Function

```
let m = Module.load("libjvm.so");

Let fn = m.enumerateSymbols().find((e) => e.name ==
  "_ZN16OldGCAllocRegion19allocate_new_regionEmb")
```

Find Function On Load

```
let m : NativePointer = Module.findExportByName(null, 'dlopen')!;

Interceptor.attach(m, { onEnter: (args) => {this.path =
args[0].readCString(); },
  onLeave: function (retval) { …🎯… }

  },

});
```

Trace!

```
let m = Module.load("./libjvm.so");

Let fn = m.enumerateSymbols().find((e) => e.name ==
  "_ZN16OldGCAllocRegion19allocate_new_regionEmb");

Interceptor.attach(fn.address, {
  onEnter(args) {
    console.log(`a_n_r word_size=${args[1]} force=${args[2]}`)
  }
});
```

Trace!

```
Spawned `java -XX:+UseG1GC -cp . MakeOldgen 1`. Resuming main
thread!

[Local::java ]-> Objects tenure after surviving 15 rounds of GC.
Running 16 rounds

a_n_r word_size=0x400 force=0x0

…

a_n_r word_size=0xffff force=0x0
```

Watch!

```
let o = m.enumerateSymbols().
        find(x=>x.name == '__frame_dummy_init_array_entry')!;

MemoryAccessMonitor.enable(
  {base:o.address, size:4096},
  {
    onAccess: (access)=>
      console.log(
              `${access.operation} ${access.address}`)})
  }
)
```

Watch!

```
frida -l x.ts -f ~/jdks/jdk8usr/bin/java -- -version

…

   . . . .   Connected to Local System (id=local)

Spawned `/usr/bin/java -version`. Resuming main thread!

[Local::java ]-> read 0x7fa996d060a0
```

Summary

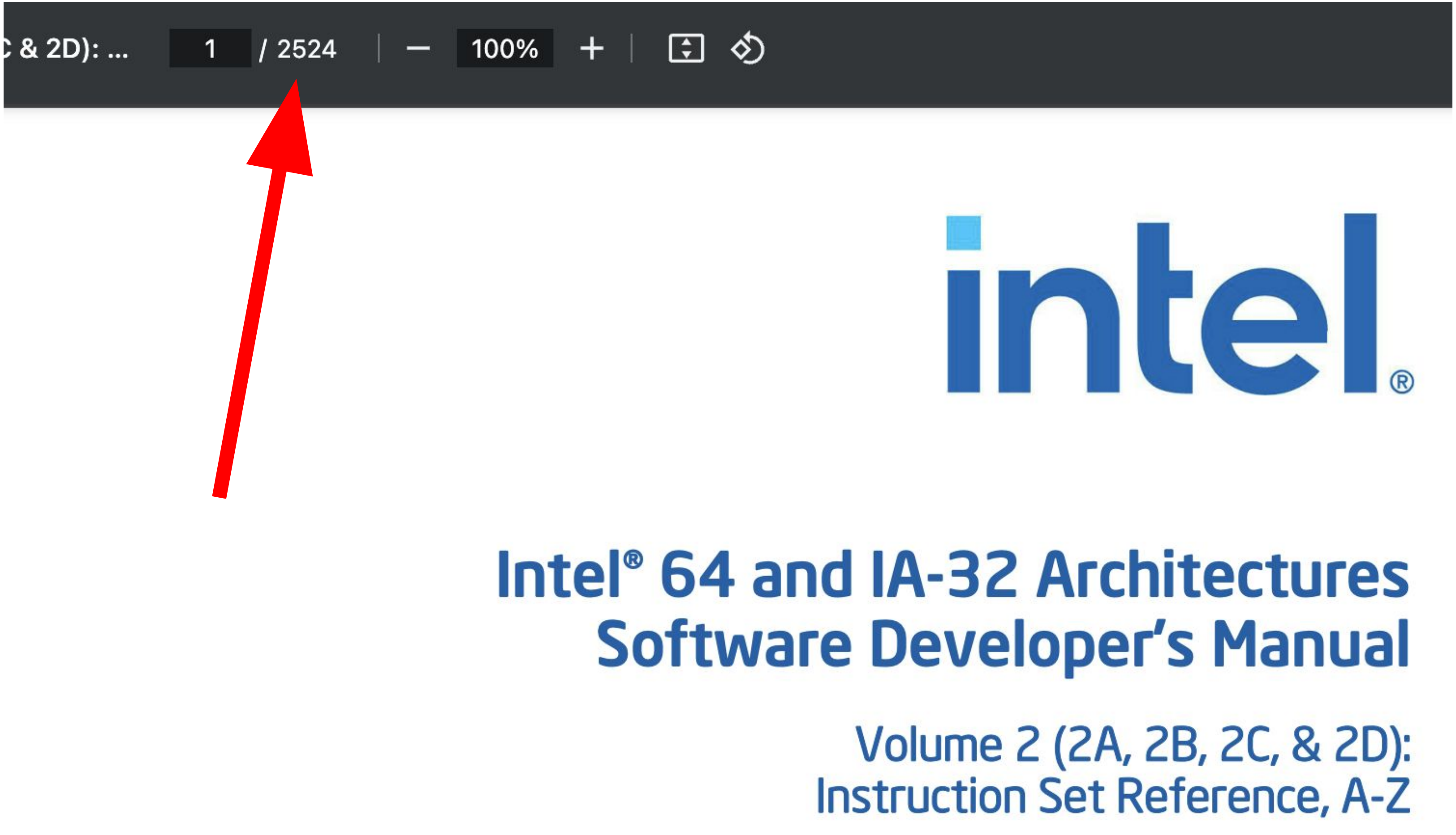
Search debug symbols and code

Plan what you need to know

Debug it with breakpoints

Decompile when optimization hits

Trace with frida for history



Intel® 64 and IA-32 Architectures Software Developer’s Manual

Volume 2 (2A, 2B, 2C, & 2D): Instruction Set Reference, A-Z