THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
EUROPE

“Goodbye ! printf()” hands-on tutorials with uftrace: function graph tracer for C/C++

Taeung Song 송태웅 , KOSSLAB

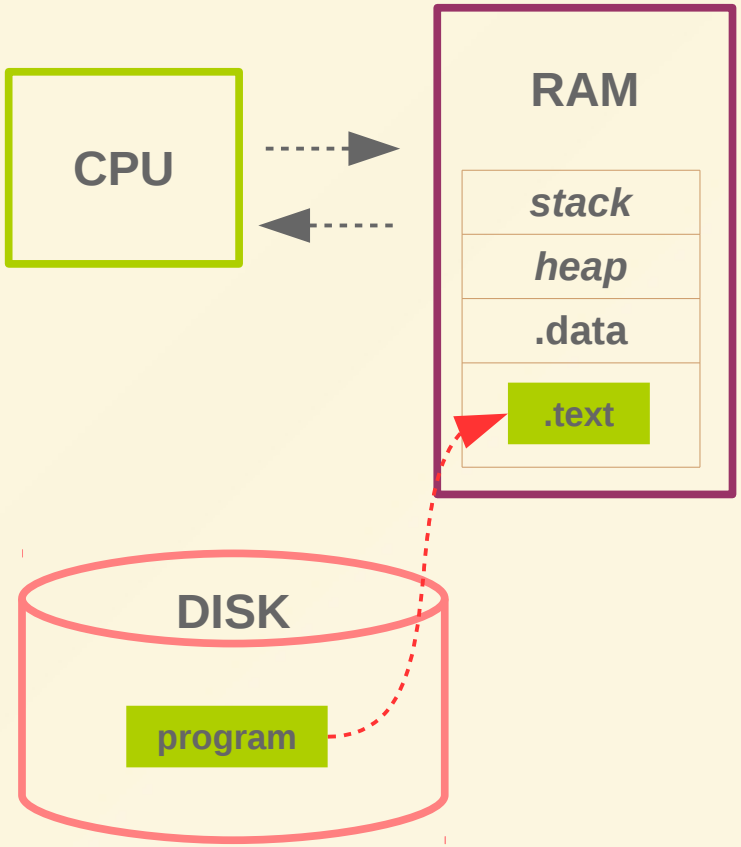
THE LINUX FOUNDATION

Why use printf() ?

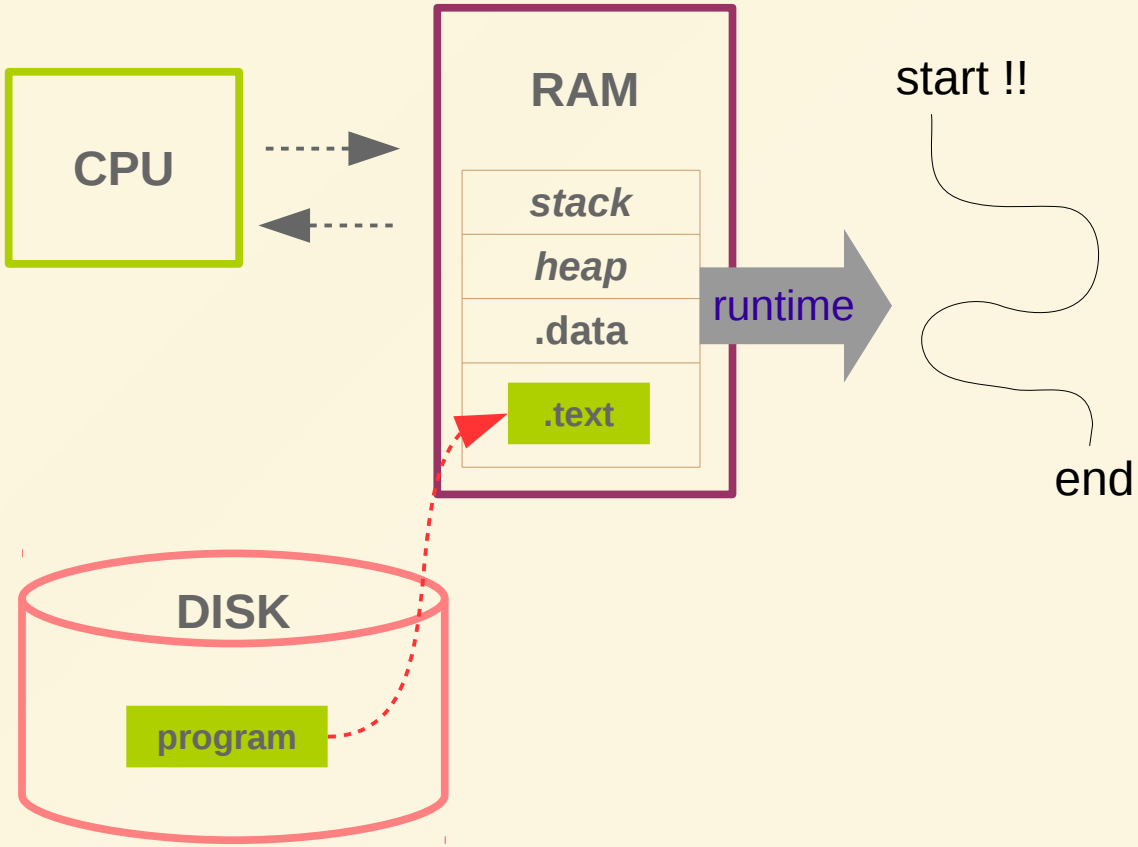
during development

As you know..

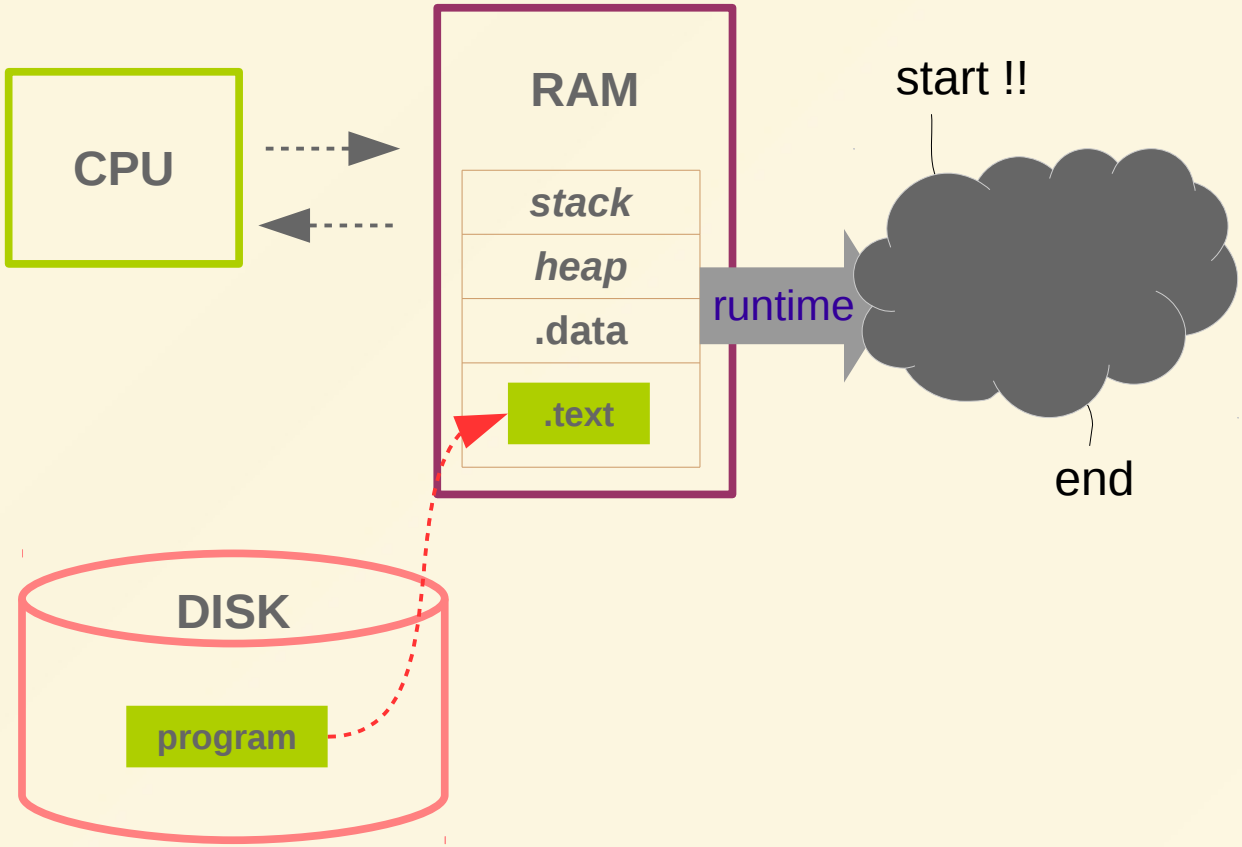
Program Execution



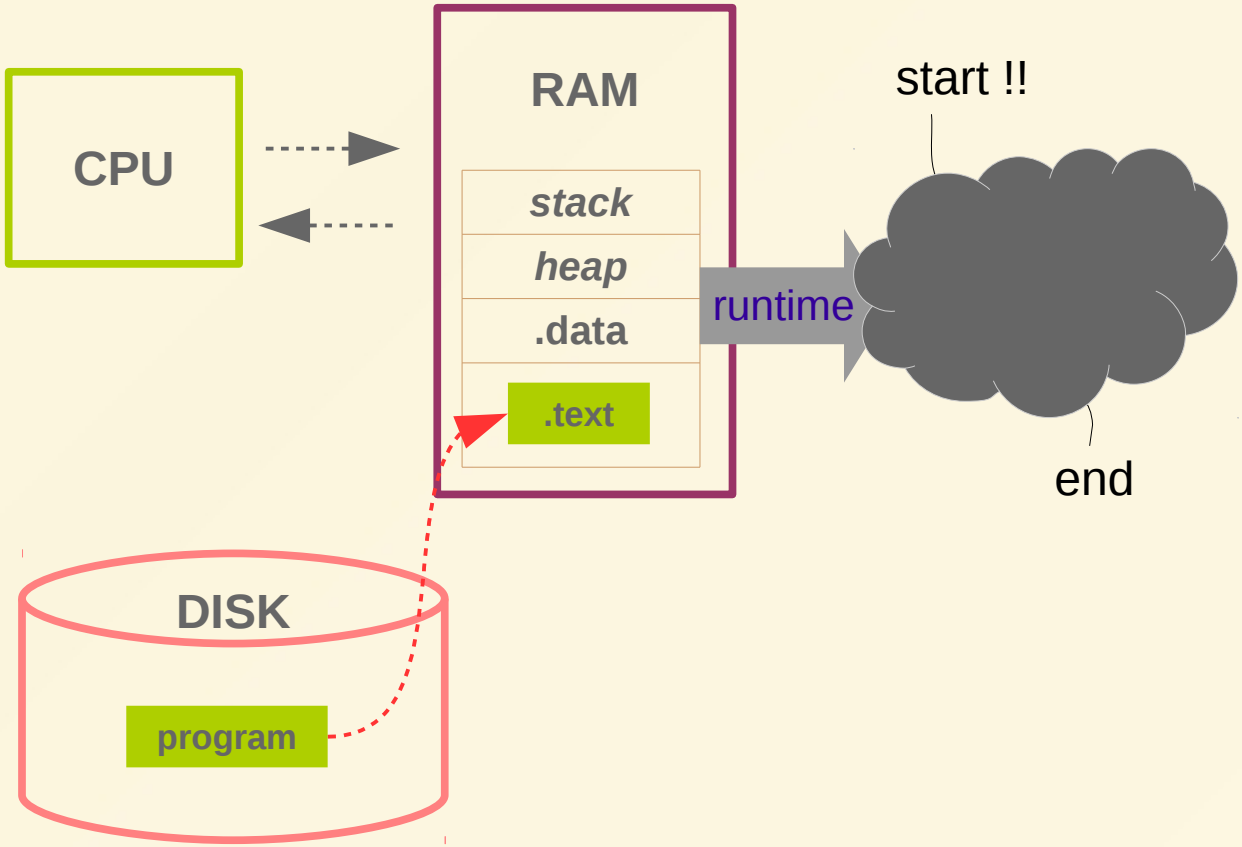
Execution Flow is



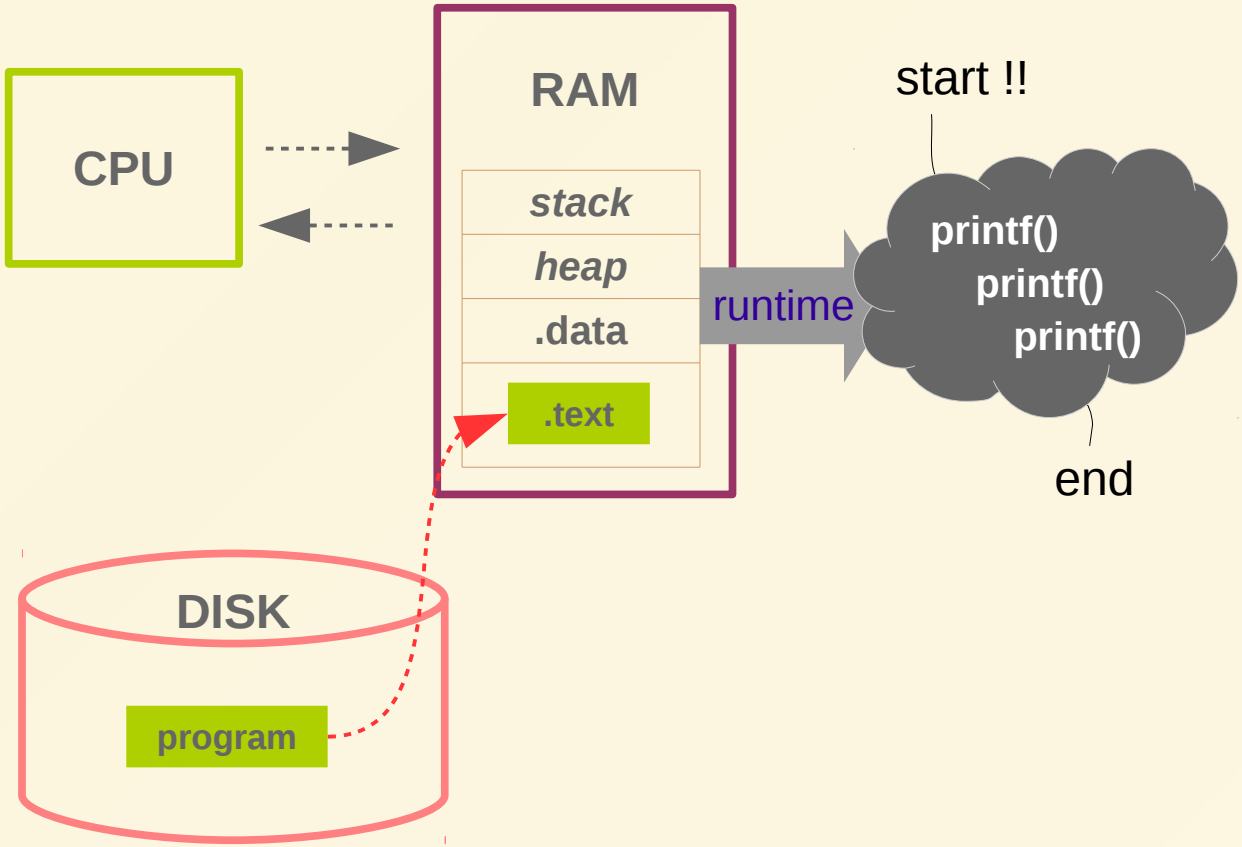
Execution Flow is invisible



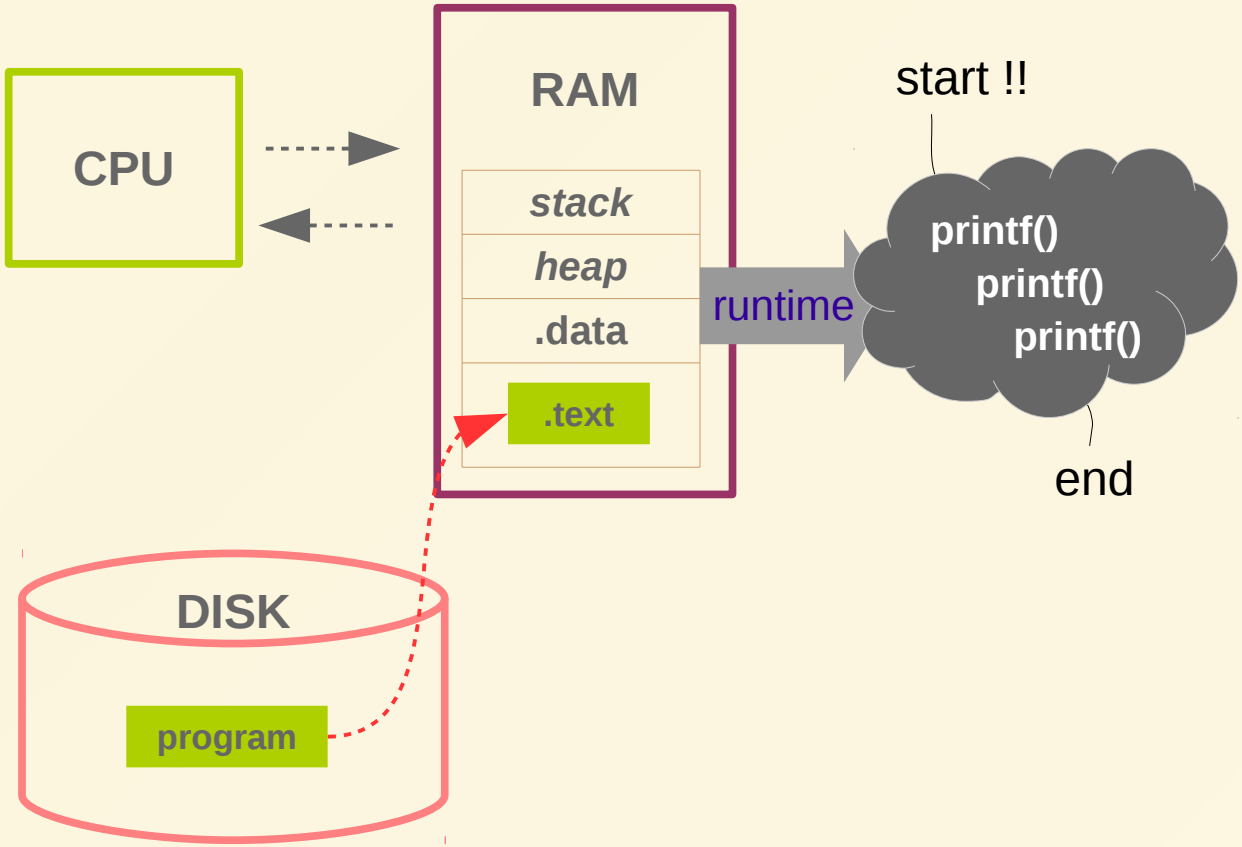
How to solve it ?



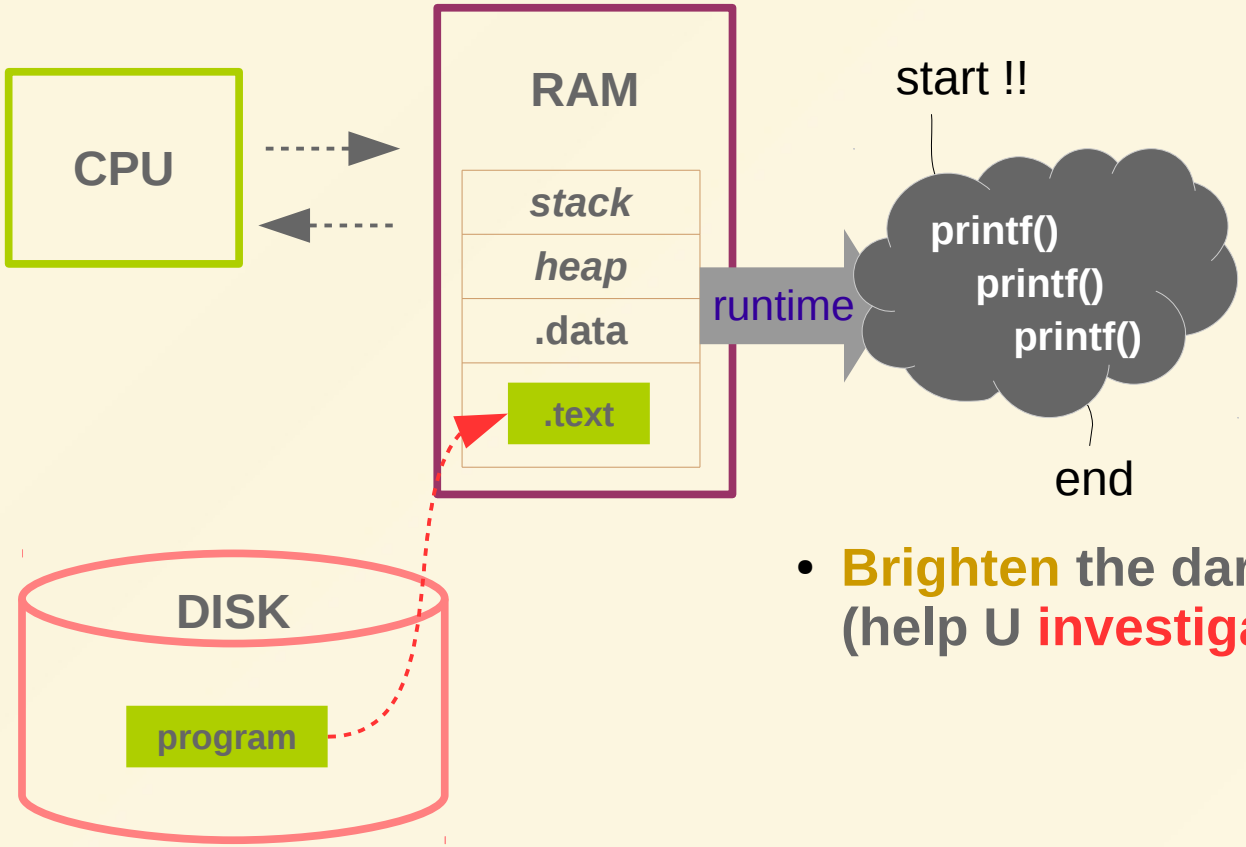
The proper solution is printf() !!



Why printf() ?

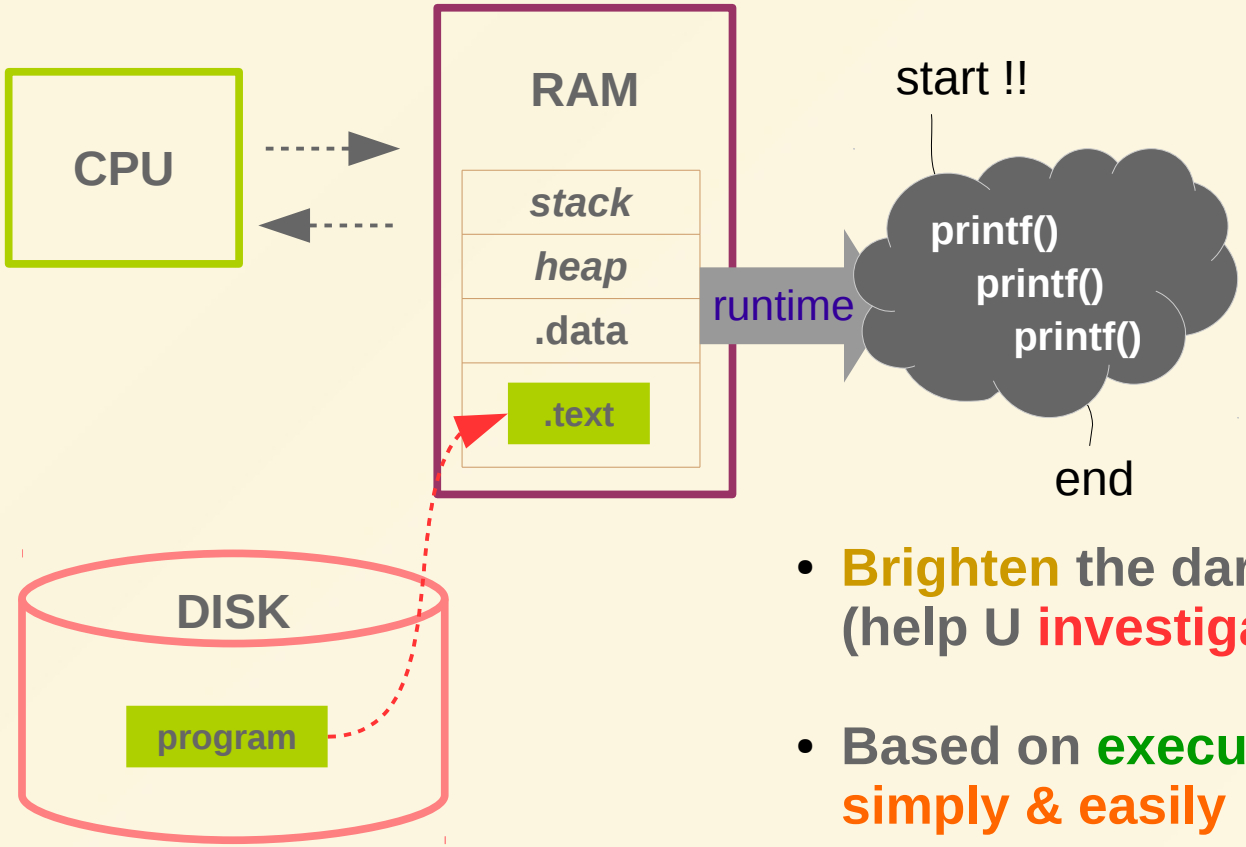

CPU
RAM
stack
heap
.data
.text
runtime
start !!
printf()
printf()
printf()
end
DISK
program

Why printf() ?



- **Brighten** the dark
  (help U **investigate** it's internals)

Why printf() ?



- **Brighten** the dark
  (help U **investigate** it's internals)
- Based on **execution flow**
  simply & easily

Benefit of printf()

- Brighten the dark of process (help U investigate internals)
- Based on execution flow simply & easily

uftrace

+α

Benefit of printf()

- Brighten the dark of process (help U investigate internals)
- Based on execution flow simply & easily

uftrace

+α : without source code modification

Benefit of printf()

- Brighten the dark of process (help U investigate internals)
- Based on execution flow simply & easily

uftrace

+α : without source code modification

+β, ...

Benefit of printf()

- Brighten the dark of process (help U investigate internals)
- Based on execution flow simply & easily

“Goodbye ! printf()”

UFTRACE

https://github.com/namhyung/uftrace

https://gitter.im/uftrace/uftrace

This repository | Search | Pull requests | Issues | Marketplace | Explore

namhyung / uftrace

Unwatch 46 | Unstar 497 | Fork 82

Code | Issues 27 | Pull requests 7 | Wiki | Insights

Function (graph) tracer for user-space

trace function tracer

2,129 commits | 24 branches | 9 releases | 14 contributors | GPL-2.0

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

namhyung Merge branch 'filter-fix' ... Latest commit d116982 2 days ago

arch	mcount: Remove a residue 'cmpq' after mcount_entry()	4 days ago
check-deps	build: Remove all executable files for check-clean	2 months ago
doc	trigger: Add "filter" and "notrace" actions	5 days ago
libmcount	filter: Allow setting filter on kernel functions	2 days ago
libtraceevent	libtraceevent: Adjust switch statements for fall-through warning on g...	6 months ago

README.md

build passing coverity passed

uftrace

The uftrace tool is to trace and analyze execution of a program written in C/C++. It was heavily inspired by the ftrace framework of the Linux kernel (especially function graph tracer) and supports userspace programs. It supports various kind of commands and filters to help analysis of the program execution and performance.

- Homepage: https://github.com/namhyung/uftrace
- Tutorial: https://github.com/namhyung/uftrace/wiki/Tutorial
- Chat: https://gitter.im/uftrace/uftrace
- Mailing list: uftrace@googlegroups.com

README.md

build passing | coverity passed

uftrace

The uftrace tool is to trace and analyze execution of a program written in C/C++. It was heavily inspired by the ftrace framework of the Linux kernel (especially function graph tracer) and supports userspace programs. It supports various kind of commands and filters to help analysis of the program execution and performance.

- Homepage: https://github.com/namhyung/uftrace
- Tutorial: https://github.com/namhyung/uftrace/wiki/Tutorial
- Chat: https://gitter.im/uftrace/uftrace
- Mailing list: uftrace@googlegroups.com

Come in and ask questions !!

Introduction to uftrace

uftrace

Function tracer for C/C++ programs

- created by Namhyung Kim
  - LG Electronics open-source contribution team
  - Linux kernel developer (since 2010)
    - perf, ftrace, …

- inspired by ftrace framework in the kernel
- **record** and **replay** model

```
$ gcc -pg -o fibonacci tests/s-fibonacci.c

$ uftrace -A fib@arg1 -R fib@retval fibonacci 5
# DURATION    TID     FUNCTION
   0.633 us [ 2851] | __monstartup();
   0.480 us [ 2851] | __cxa_atexit();
            [ 2851] | main() {
   0.546 us [ 2851] |   atoi();
            [ 2851] |   fib(5) {
            [ 2851] |     fib(4) {
            [ 2851] |       fib(3) {
   1.146 us [ 2851] |         fib(2) = 1;
   0.077 us [ 2851] |         fib(1) = 1;
   1.823 us [ 2851] |       } = 2; /* fib */
   0.062 us [ 2851] |       fib(2) = 1;
   2.199 us [ 2851] |     } = 3; /* fib */
            [ 2851] |     fib(3) {
   0.061 us [ 2851] |       fib(2) = 1;
   0.067 us [ 2851] |       fib(1) = 1;
   0.474 us [ 2851] |     } = 2; /* fib */
   3.317 us [ 2851] |   } = 5; /* fib */
   4.343 us [ 2851] | } /* main */
```

uftrace

“C/C++ execution flow”

```
# Default == record + replay

$ uftrace -A fib@arg1 -R fib@retval fibonacci 5
# DURATION    TID     FUNCTION
   0.633 us [ 2851] | __monstartup();
   0.480 us [ 2851] | __cxa_atexit();
            [ 2851] | main() {
   0.546 us [ 2851] |   atoi();
            [ 2851] |   fib(5) {
            [ 2851] |     fib(4) {
            [ 2851] |       fib(3) {
   1.146 us [ 2851] |         fib(2) = 1;
   0.077 us [ 2851] |         fib(1) = 1;
   1.823 us [ 2851] |       } = 2; /* fib */
   0.062 us [ 2851] |       fib(2) = 1;
   2.199 us [ 2851] |     } = 3; /* fib */
            [ 2851] |     fib(3) {
   0.061 us [ 2851] |       fib(2) = 1;
   0.067 us [ 2851] |       fib(1) = 1;
   0.474 us [ 2851] |     } = 2; /* fib */
   3.317 us [ 2851] |   } = 5; /* fib */
   4.343 us [ 2851] | } /* main */
```

uftrace

“C/C++ execution flow”

Function Call Trace

```
# Default == record + replay

$ uftrace -A fib@arg1 -R fib@retval fibonacci 5
# DURATION     TID     FUNCTION
   0.633 us [ 2851] | __monstartup();
   0.480 us [ 2851] | __cxa_atexit();
            [ 2851] | main() {
   0.546 us [ 2851] |   atoi();
            [ 2851] |   fib(5) {
            [ 2851] |     fib(4) {
            [ 2851] |       fib(3) {
   1.146 us [ 2851] |         fib(2) = 1;
   0.077 us [ 2851] |         fib(1) = 1;
   1.823 us [ 2851] |       } = 2; /* fib */
   0.062 us [ 2851] |       fib(2) = 1;
   2.199 us [ 2851] |     } = 3; /* fib */
            [ 2851] |     fib(3) {
   0.061 us [ 2851] |       fib(2) = 1;
   0.067 us [ 2851] |       fib(1) = 1;
   0.474 us [ 2851] |     } = 2; /* fib */
   3.317 us [ 2851] |   } = 5; /* fib */
   4.343 us [ 2851] | } /* main */
```

uftrace

“C/C++ each function

Execution time”

```
# Default == record + replay

$ uftrace -A fib@arg1 -R fib@retval fibonacci 5
# DURATION     TID     FUNCTION
   0.633 us [ 2851] | __monstartup();
   0.480 us [ 2851] | __cxa_atexit();
            [ 2851] | main() {
   0.546 us [ 2851] |   atoi();
            [ 2851] |   fib(5) {
            [ 2851] |     fib(4) {
            [ 2851] |       fib(3) {
   1.146 us [ 2851] |         fib(2) = 1;
   0.077 us [ 2851] |         fib(1) = 1;
   1.823 us [ 2851] |       } = 2; /* fib */
   0.062 us [ 2851] |       fib(2) = 1;
   2.199 us [ 2851] |     } = 3; /* fib */
            [ 2851] |     fib(3) {
   0.061 us [ 2851] |       fib(2) = 1;
   0.067 us [ 2851] |       fib(1) = 1;
   0.474 us [ 2851] |     } = 2; /* fib */
   3.317 us [ 2851] |   } = 5; /* fib */
   4.343 us [ 2851] | } /* main */
```

uftrace

"Arguments"

based on
Function Call Trace

```
# Default == record + replay

$ uftrace -A fib@arg1 -R fib@retval fibonacci 5
# DURATION     TID     FUNCTION
   0.633 us [ 2851] | __monstartup();
   0.480 us [ 2851] | __cxa_atexit();
            [ 2851] | main() {
   0.546 us [ 2851] |   atoi();
            [ 2851] |   fib(5) {
            [ 2851] |     fib(4) {
            [ 2851] |       fib(3) {
   1.146 us [ 2851] |         fib(2) = 1;
   0.077 us [ 2851] |         fib(1) = 1;
   1.823 us [ 2851] |       } = 2; /* fib */
   0.062 us [ 2851] |       fib(2) = 1;
   2.199 us [ 2851] |     } = 3; /* fib */
            [ 2851] |     fib(3) {
   0.061 us [ 2851] |       fib(2) = 1;
   0.067 us [ 2851] |       fib(1) = 1;
   0.474 us [ 2851] |     } = 2; /* fib */
   3.317 us [ 2851] |   } = 5; /* fib */
   4.343 us [ 2851] | } /* main */
```

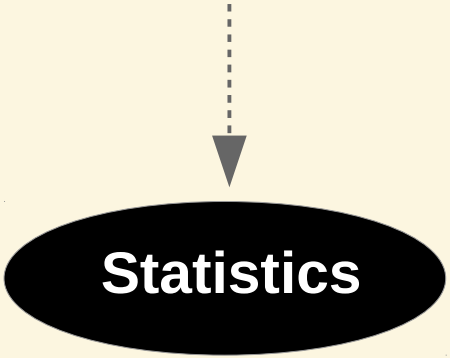
uftrace

“Return values”

based on
Function Call Trace

```
$ uftrace record fibonacci 5

$ uftrace report -s call

  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ============
    1.400 us    1.400 us           9  fib
    0.398 us    0.398 us           1  __cxa_atexit
    0.489 us    0.489 us           1  __monstartup
    0.603 us    0.603 us           1  atoi
    2.454 us    0.451 us           1  main
```

uftrace report

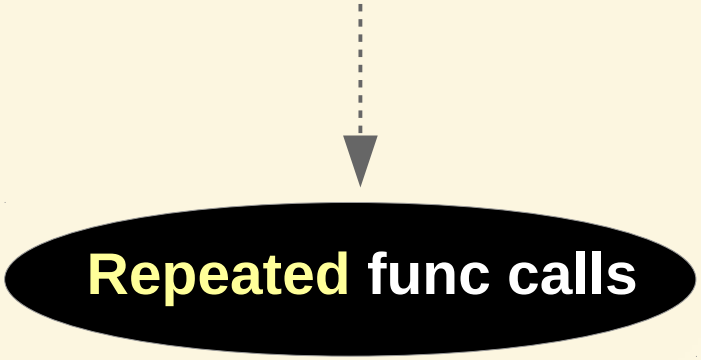


“Duration (time)”

“Function call counts”

```
$ uftrace record fibonacci 5

$ uftrace graph
#
# function graph for 'main' (session:
58de6d06edafbe8d)
#

backtrace
=====================================
 backtrace #0: hit 1, time   2.454 us
   [0] main (0x4006d6)

calling functions
=====================================
   2.454 us : (1) main
   0.603 us :  +-(1) atoi
            :  |
   1.400 us :  +-(1) fib
   1.161 us :    (2) fib
   0.681 us :    (4) fib
   0.139 us :    (2) fib
```

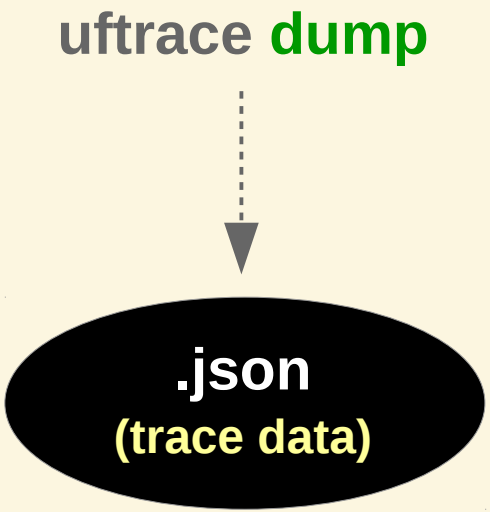
uftrace graph



“Total time”

“Hit counts”

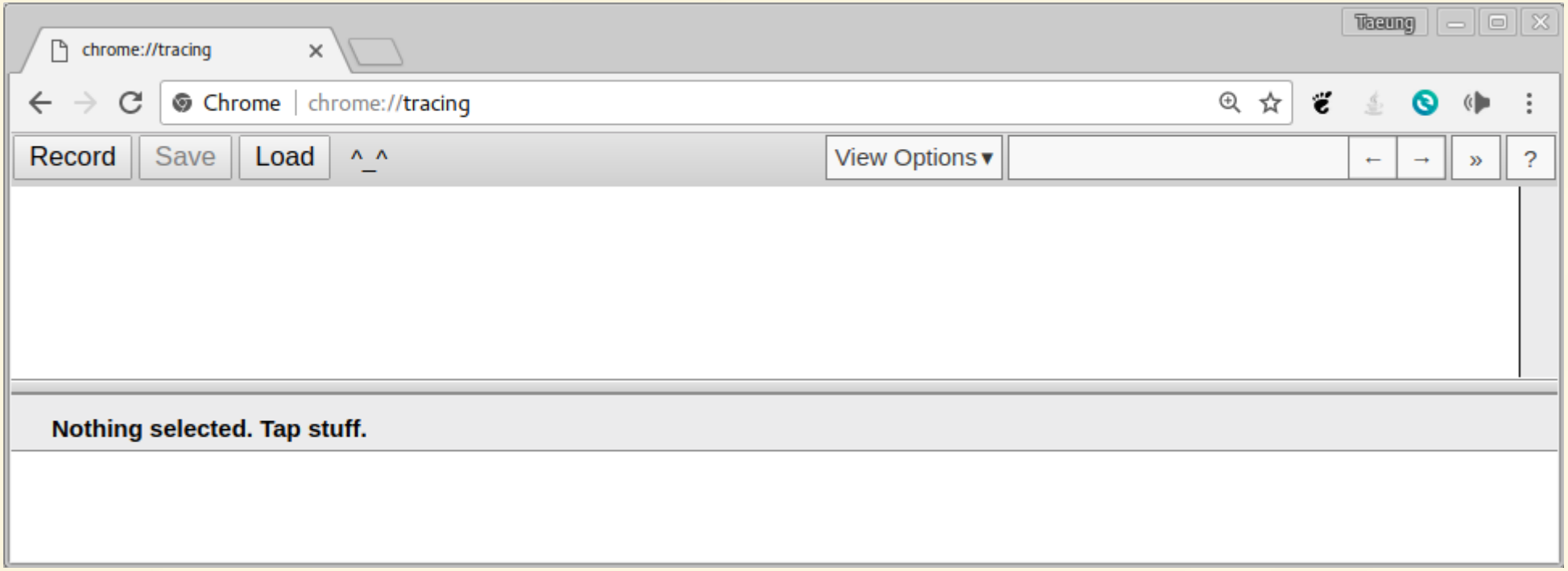
```
$ uftrace dump --chrome
{"traceEvents":[
{"ts":326310414447.272,"ph":"B","pid":11326,"name":"__monstartup"},
{"ts":326310414447.761,"ph":"E","pid":11326,"name":"__monstartup"},
{"ts":326310414449.567,"ph":"B","pid":11326,"name":"__cxa_atexit"},
{"ts":326310414449.965,"ph":"E","pid":11326,"name":"__cxa_atexit"},
{"ts":326310414450.491,"ph":"B","pid":11326,"name":"main"},
{"ts":326310414450.588,"ph":"B","pid":11326,"name":"atoi"},
{"ts":326310414451.191,"ph":"E","pid":11326,"name":"atoi"},
{"ts":326310414451.455,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414451.547,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414451.590,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414451.632,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414451.719,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414451.956,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414452.008,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.123,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.227,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414452.275,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.355,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.425,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414452.484,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414452.536,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.673,"ph":"B","pid":11326,"name":"fib"},
{"ts":326310414452.721,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.778,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.855,"ph":"E","pid":11326,"name":"fib"},
{"ts":326310414452.945,"ph":"E","pid":11326,"name":"main"}
], "displayTimeUnit": "ns", "metadata": {
"command_line":"uftrace record ./fibonacci 5 ",
"recorded_time":"Thu Oct 19 06:03:54 2017"
} }
```



```
$ uftrace dump --chrome > fibonacci.json

$ google-chrome
```

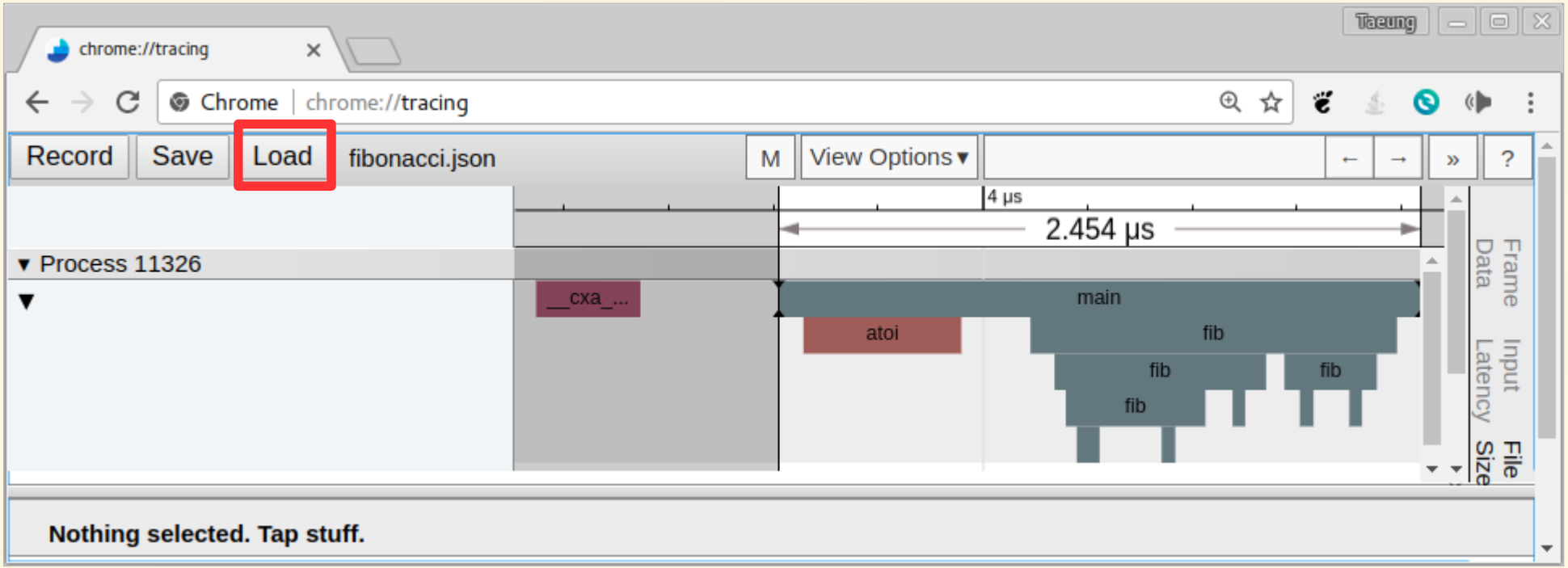
```
$ uftrace dump --chrome > fibonacci.json

$ google-chrome
```

chrome://tracing →



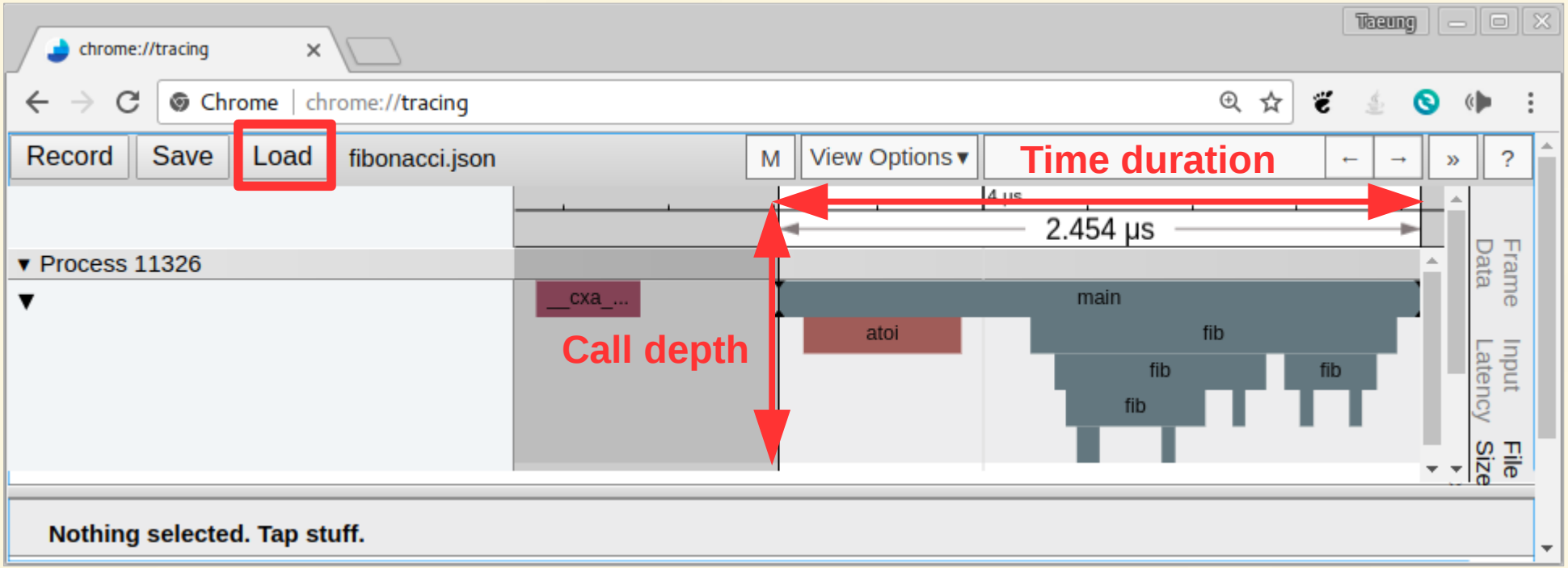
```
$ uftrace dump --chrome > fibonacci.json

$ google-chrome
```

chrome://tracing → Load → fibonacci.json → Function call graph



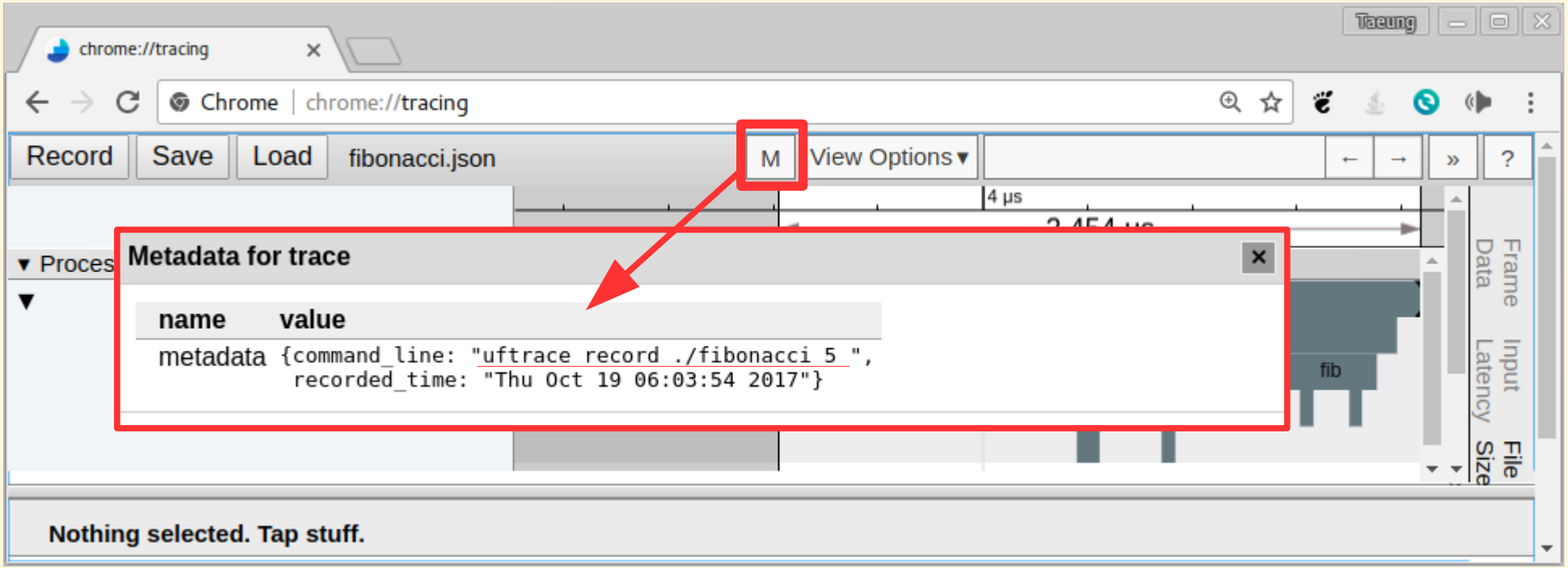
```
$ uftrace dump --chrome > fibonacci.json

$ google-chrome
```

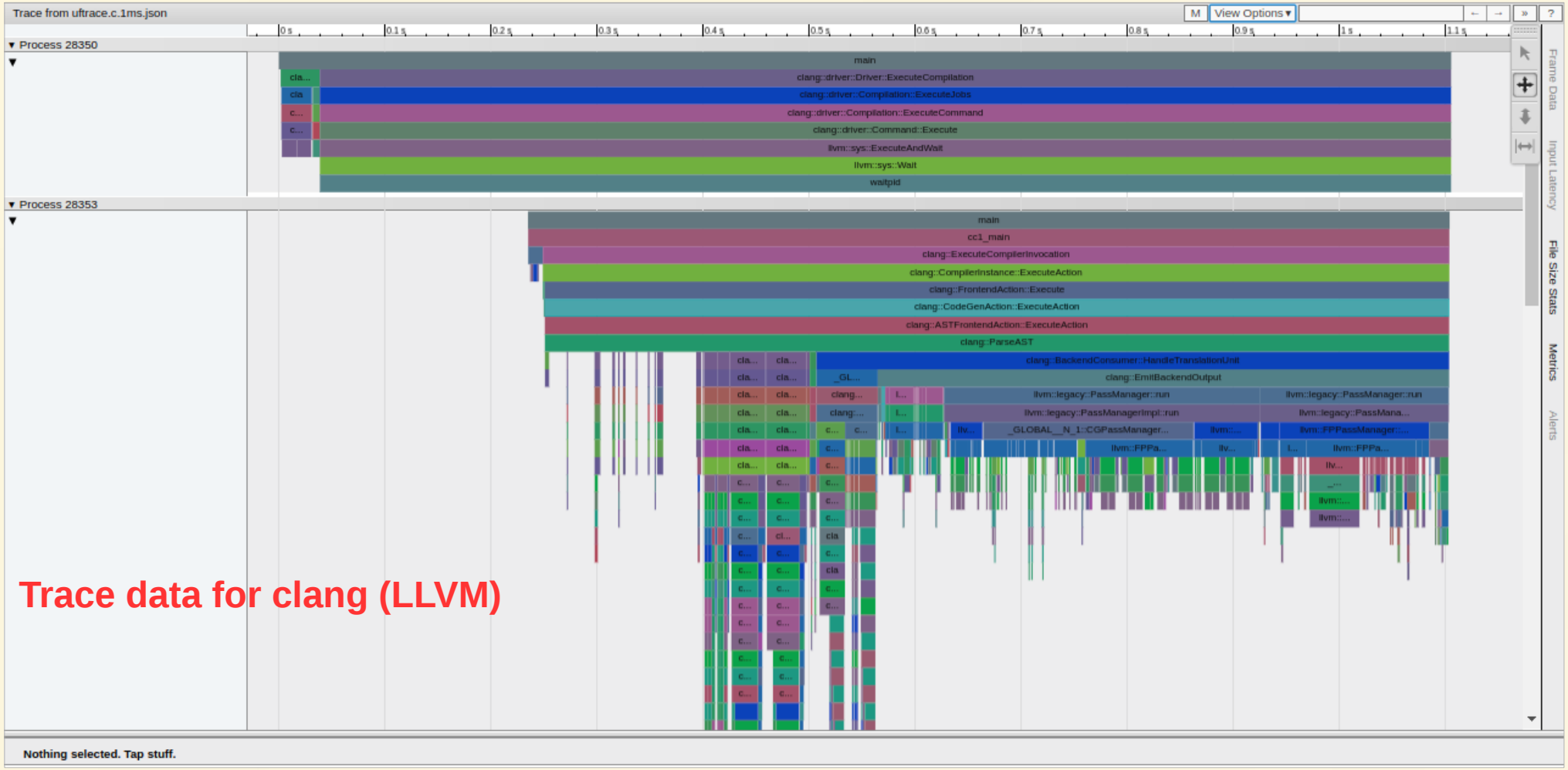
chrome://tracing → Load → fibonacci.json → Function call graph



```
$ uftrace dump --chrome > fibonacci.json

$ google-chrome
```

chrome://tracing → Load → fibonacci.json → Function call graph





Trace data for clang (LLVM)

https://honggyukim.github.io/uftrace/clang/uftrace.c.html

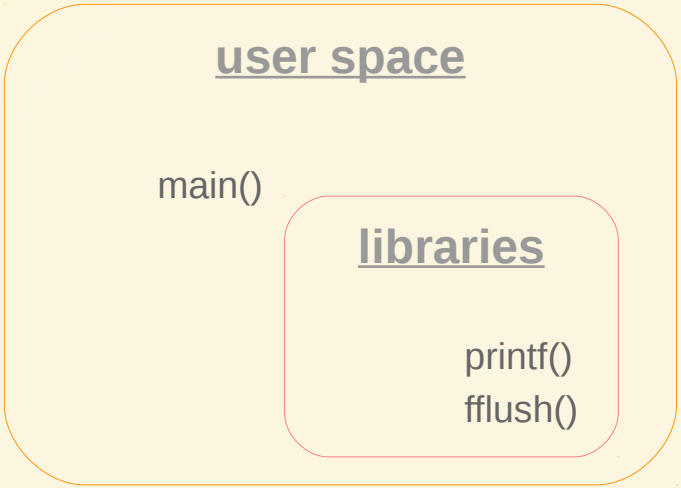
uftrace can trace User + Lib + Kernel

showing the execution flow

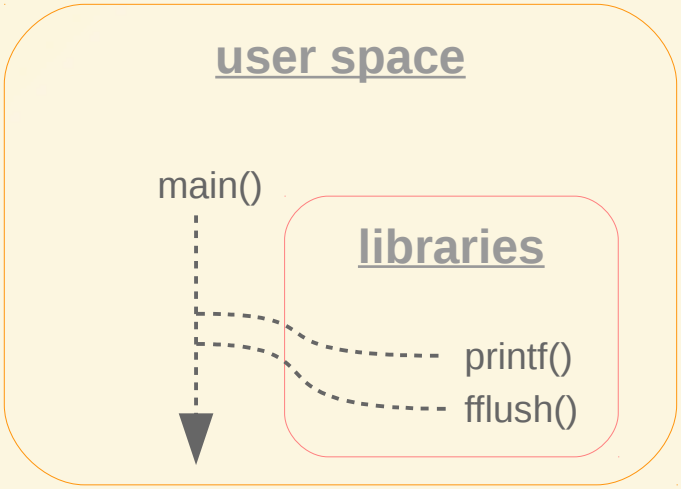
uftrace = user function trace
+ strace + ltrace + ftrace

based on the execution flow

```
$ uftrace record hello
Hello OSSEU17 !!

$ uftrace replay
# DURATION    TID     FUNCTION
   0.710 us [13588] | __monstartup();
   0.713 us [13588] | __cxa_atexit();
            [13588] | main() {
   4.107 us [13588] |   printf();
   4.046 us [13588] |   fflush();
   8.815 us [13588] | } /* main */
```

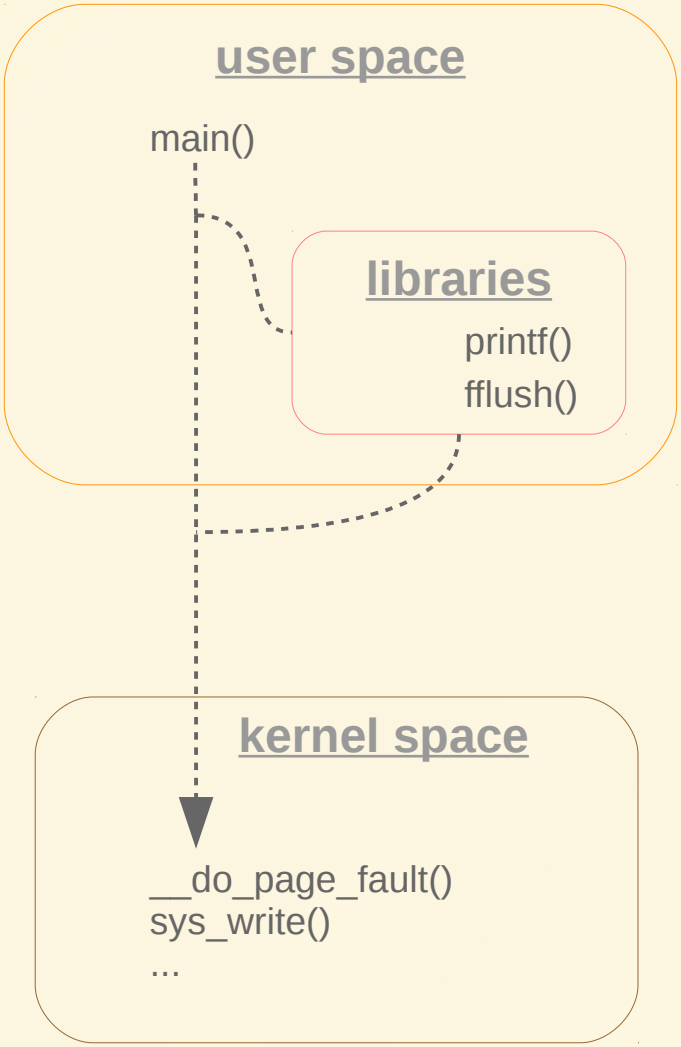


```
$ uftrace record hello
Hello OSSEU17 !!

$ uftrace replay
# DURATION    TID     FUNCTION
   0.710 us [13588] | __monstartup();
   0.713 us [13588] | __cxa_atexit();
            [13588] | main() {
   4.107 us [13588] |   printf();
   4.046 us [13588] |   fflush();
   8.815 us [13588] | } /* main */
```

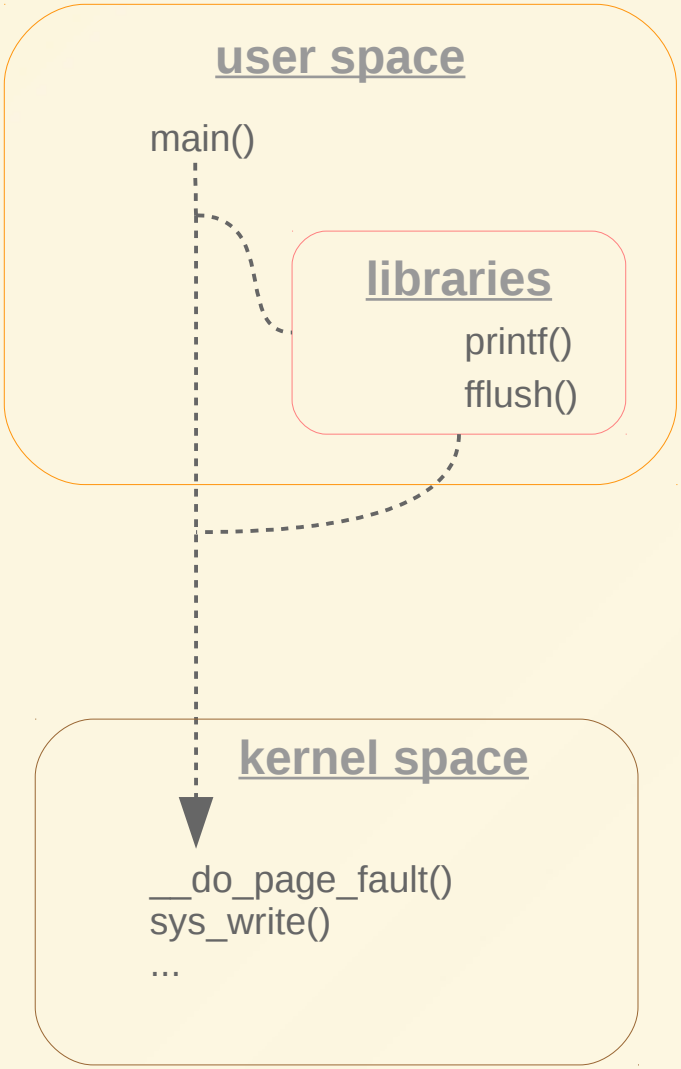


```
$ uftrace record -k hello
Hello OSSEU17 !!

$ uftrace replay
# DURATION    TID     FUNCTION
   1.060 us [13565] | __monstartup();
   1.113 us [13565] | __cxa_atexit();
            [13565] | main() {
            [13565] |   printf() {
   3.173 us [13565] |     sys_newfstat();
   6.107 us [13565] |     __do_page_fault();
  17.713 us [13565] |   } /* printf */
            [13565] |   fflush() {
   7.198 us [13565] |     sys_write();
  12.270 us [13565] |   } /* fflush */
  30.661 us [13565] | } /* main */
```

Integrated tracer !



```
$ uftrace record -K 2 hello
Hello OSSEU17 !!

$ uftrace replay
# DURATION    TID     FUNCTION
   0.887 us [17099] | __monstartup();
   1.039 us [17099] | __cxa_atexit();
            [17099] | main() {
            [17099] |   printf() {
            [17099] |     sys_newfstat() {
   1.378 us [17099] |       vfs_fstat();
   0.561 us [17099] |       cp_new_stat();
   4.197 us [17099] |     } /* sys_newfstat */
            [17099] |     __do_page_fault() {
   0.233 us [17099] |       down_read_trylock();
   0.239 us [17099] |       _cond_resched();
   1.839 us [17099] |       find_vma();
   6.288 us [17099] |       handle_mm_fault();
   0.249 us [17099] |       up_read();
  10.514 us [17099] |     } /* __do_page_fault */
  22.183 us [17099] |   } /* printf */
            [17099] |   fflush() {
            [17099] |     sys_write() {
   0.772 us [17099] |       __fdget_pos();
   7.731 us [17099] |       vfs_write();
  11.184 us [17099] |     } /* sys_write */
  15.619 us [17099] |   } /* fflush */
  38.504 us [17099] | } /* main */
```



uftrace

Features

- C/C++ (user space) functions
  - compiled with **-pg** or -finstrument-functions
- Library functions
- Linux kernel functions
- Some of system events
  - schedule in-out
  - page faults

uftrace Installation

```
# Ubuntu
$ sudo apt-get install libelf-dev

# Fedora, RHEL
$ sudo dnf install elfutils-libelf-devel
```

DEPENDENCY

Need to install libelf

```
# Ubuntu
$ sudo apt-get install libelf-dev

# Fedora, RHEL
$ sudo dnf install elfutils-libelf-devel


$ git clone https://github.com/namhyung/uftrace.git

$ cd uftrace
```

GETTING THE SOURCE

Need to git-clone

```
# Ubuntu
$ sudo apt-get install libelf-dev

# Fedora, RHEL
$ sudo dnf install elfutils-libelf-devel


$ git clone https://github.com/namhyung/uftrace.git

$ cd uftrace


$ ./configure

$ make

$ sudo make install
```

BUILD

Need to **make**

```
$ cd uftrace

# You can check many test source files
$ cd tests/ && ls s-*
```

TEST

Various test cases

```
$ cd uftrace

# You can check many test source files
$ cd tests/ && ls s-*



# For example, you can run the 090 test case
$ ./runtest.py 090

# Or, you can run it by yourself
$ gcc -pg -o fib s-fibonacci.c

$ uftrace ./fib
```

TEST

Various test cases

Live demo

fibonacci example

Live demo

fibonacci example

Step by step, together !!

uftrace tutorials

https://github.com/taeung/uftrace-osseu17

https://github.com/taeung/uftrace-osseu17

Get uftrace tutorial examples

https://github.com/taeung/uftrace-osseu17

Get uftrace tutorial examples

recorded data by uftrace

Reproduce execution flow of examples,

Reproduce execution flow of **examples**,

with **recorded data** (e.g. uftrace.data)

```
$ git clone https://github.com/taeung/uftrace-osseu17.git

$ cd uftrace-osseu17/

$ ls
chrome_tracing_examples
cpython_example
Good_bye_printf_hands_on_tutorial_uftrace<...>.pdf
nmap_examples
nullptr_exception_example
optimization_level_examples
printf_kern_examples
process_life_cycle_example
```

git-clone

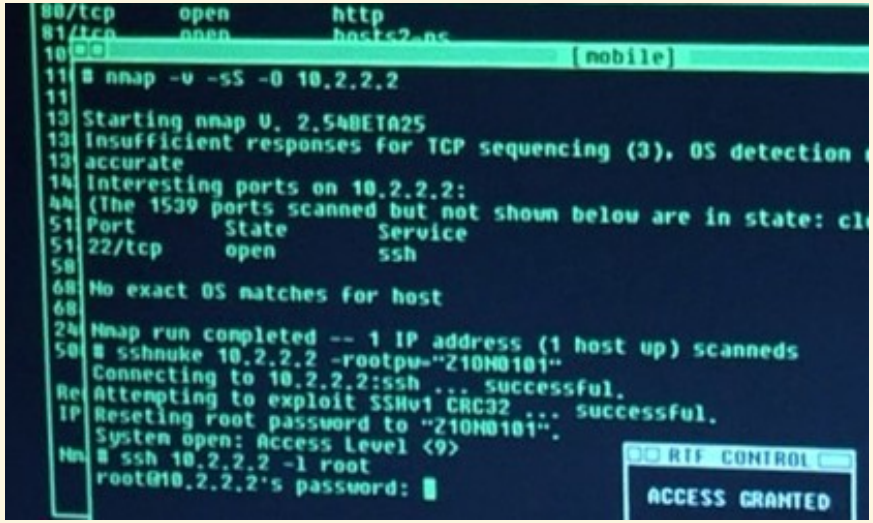
uftrace examples !!

Nmap examples

What is Nmap ?

The Matrix Reloaded (2003)

Trinitiy uses Nmap !



https://nmap.org/movies “Trinity hacking scene”

Let’s trace **Nmap** !

```
$ git clone https://github.com/nmap/nmap.git

$ cd nmap

$ ./configure

$ make
```

GETTING SRC & BUILD

But you don’t need to do

because of example files

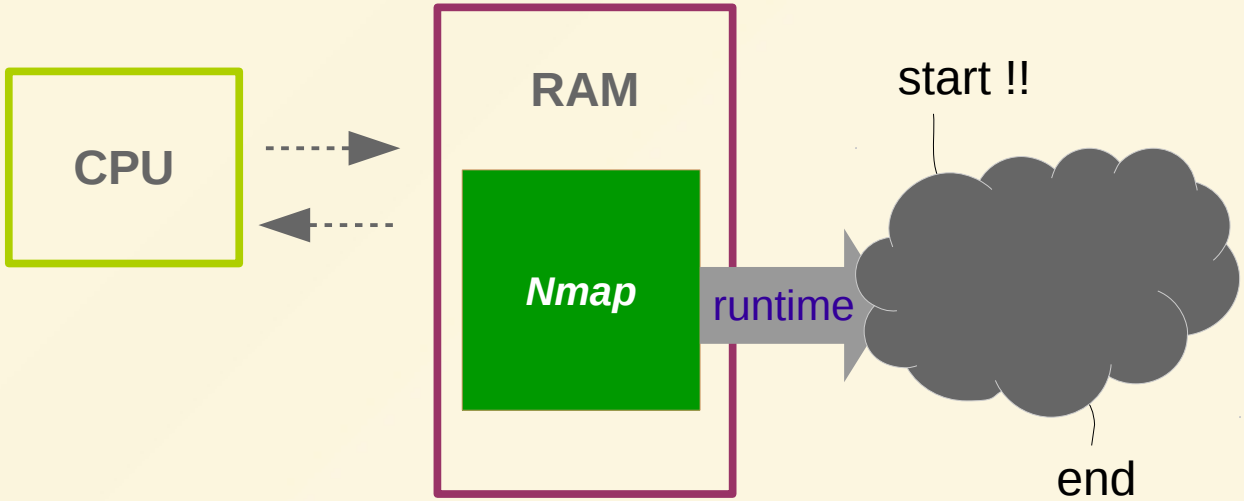
```
$ ./nmap nmap.org

Starting Nmap 7.60SVN ( https://nmap.org ) at 2017-10-19 ...
Nmap scan report for nmap.org (45.33.49.119)
Host is up (0.18s latency).
Other addresses for nmap.org (not scanned):
2600:3c01::f03c:91ff:fe98:ff4e
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
25/tcp    open   smtp
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 12.13 seconds
```

SIMPLE TEST

Nmap can port scan

https://nmap.org

How does Nmap scan port numbers?

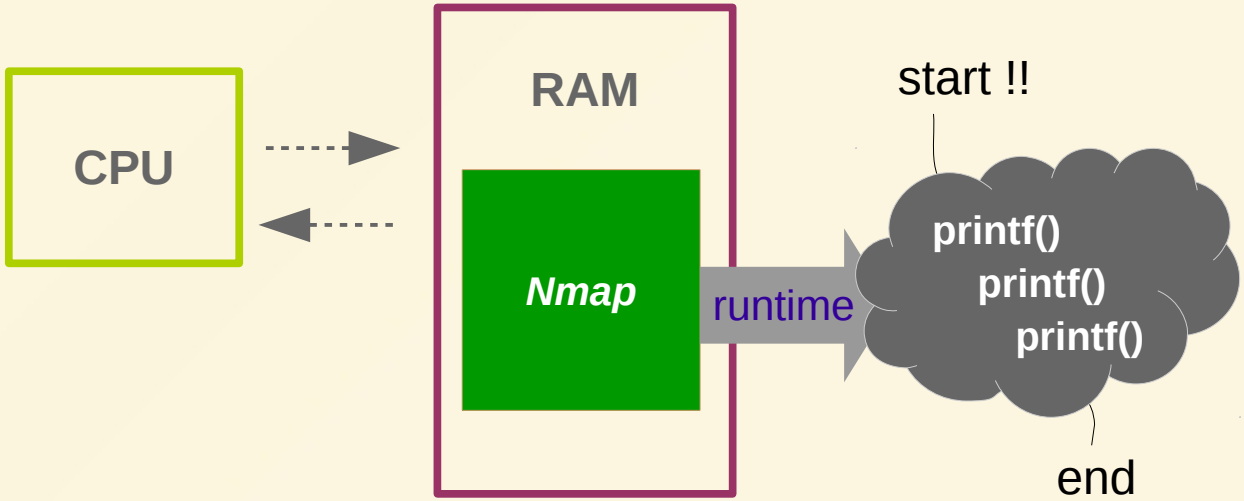


Hum..

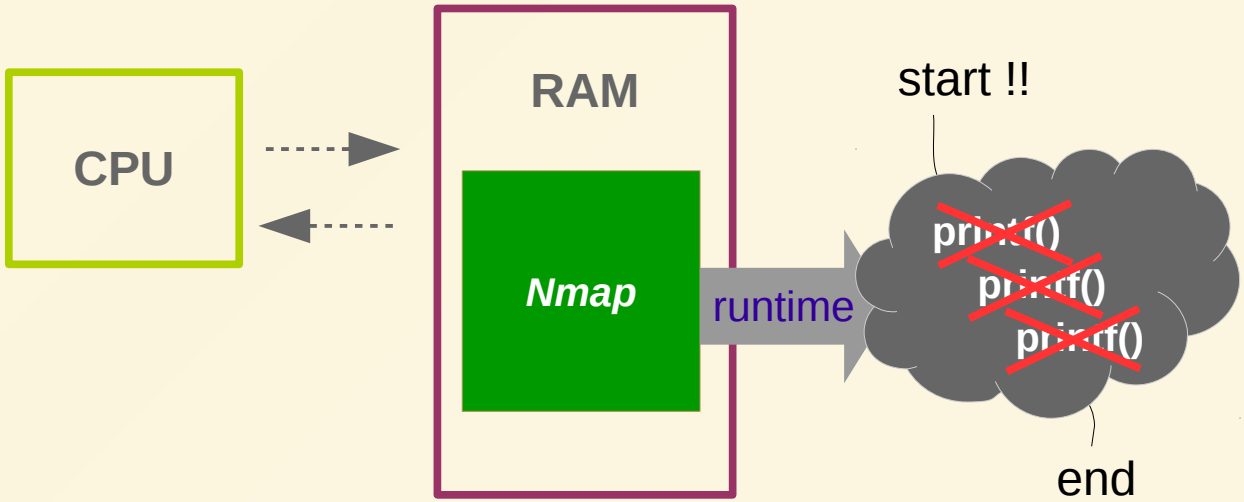
Nmap scans ports in order ?

0, 1, 2, … 65535 (16 bit unsigned int)

To investigate it, we can read Nmap src and dig using printf() !



You can use uftrace instead



You can more efficiently analyze it

You can more efficiently analyze it using uftrace !!

Let’s do it ! step by step

Step 1. Recompile Nmap

with -pg or -finstrument-functions

```
$ cd nmap/

$ emacs Makefile

$ diff Makefile.old Makefile
--- Makefile.old 2017-10-21 04:02:58.016974789 +0900
+++ Makefile     2017-10-21 04:03:10.861083599 +0900
@@ -47,9 +47,9 @@ # Level 1 only makes changes that don't
 # For mtrace debugging -- see MTRACE define in main.cc for
instructions
 # Should only be enabled during debugging and not in any real
release.
 # DEFS += -DMTRACE=1
-CXXFLAGS = -g -O2 -Wall -fno-strict-aliasing $(DBGFLAGS) $(CCOPT)
+CXXFLAGS = -pg -g -O2 -Wall -fno-strict-aliasing $(DBGFLAGS) $(CCOPT)
 CPPFLAGS = -I$(top_srcdir)/liblinear -I$(top_srcdir)/liblua -I$
(top_srcdir)/libdnet-stripped/include -I$(top_srcdir)/libssh2/include
-I$(top_srcdir)/libpcap -I$(top_srcdir)/nbase -I$
(top_srcdir)/nsock/include $(DEFS)
-CFLAGS = -g -O2 -Wall $(DBGFLAGS) $(CCOPT)
+CFLAGS = -pg -g -O2 -Wall $(DBGFLAGS) $(CCOPT)
 STATIC =
 LDFLAGS = -Wl,-E  -Lnbase -Lnsock/src/ $(DBGFLAGS) $(STATIC)
 LIBS =  -lnsock -lnbase -lpcre $(LIBPCAPDIR)/libpcap.a $
(LIBSSH2_LIBS) $(OPENSSL_LIBS) $(ZLIB_LIBS) libnetutil/libnetutil.a $
(top_srcdir)/libdnet-stripped/src/.libs/libdnet.a $
(top_srcdir)/liblua/liblua.a $(top_srcdir)/liblinear/liblinear.a -ldl

$ make
```

RECOMPILE

with -pg or

-finstrument-functions

Step 2. Nmap record & replay

in 2 ~3 depth level

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/
```

Just use recorded data !!

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace info

# system information
# ==================
# program version     : uftrace v0.8-59-g7181
# recorded on         : Fri Oct 20 13:20:03 2017
# cmdline             : uftrace record -t 5us -d uftrace.data.nmap_nmap.org ./nmap nmap.org
# cpu info            : Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz
# number of cpus      : 4 / 4 (online / possible)
# memory info         : 0.1 / 7.4 GB (free / total)
# system load         : 0.12 / 0.24 / 0.34 (1 / 5 / 15 min)
# kernel version      : Linux 4.5.0-rc4+
# hostname            : taeung-ThinkPad-X1-Carbon-3rd
# distro              : "Ubuntu 16.04.3 LTS"
#
# process information
# ===================
# number of tasks     : 1
# task list           : 7673
# exe image           : /home/taeung/git/opensource/nmap/nmap
...
```

info - read Info documents

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace info

# system information
# ==================
# program version     : uftrace v0.8-59-g7181
# recorded on         : Fri Oct 20 13:20:03 2017
# cmdline             : uftrace record -t 5us -d uftrace.data.nmap_nmap.org ./nmap nmap.org
# cpu info            : Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz
# number of cpus      : 4 / 4 (online / possible)
# memory info         : 0.1 / 7.4 GB (free / total)
# system load         : 0.12 / 0.24 / 0.34 (1 / 5 / 15 min)
# kernel version      : Linux 4.5.0-rc4+
# hostname            : taeung-ThinkPad-X1-Carbon-3rd
# distro              : "Ubuntu 16.04.3 LTS"
#
# process information
# ===================
# number of tasks     : 1
# task list           : 7673
# exe image           : /home/taeung/git/opensource/nmap/nmap
...
```

Check record cmdline !

info - read Info documents

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace replay -D 2
# DURATION    TID     FUNCTION
            [ 7673] | _GLOBAL__sub_I__ZN3DNS7Factory13progressiveIdE() {
   7.245 us [ 7673] |   open();
  21.938 us [ 7673] |   read();
  59.669 us [ 7673] | } /* _GLOBAL__sub_I__ZN3DNS7Factory13progressiveIdE */
   6.125 us [ 7673] | _GLOBAL__sub_I__Z16set_program_namePKc();
            [ 7673] | _GLOBAL__sub_I_o() {
   5.718 us [ 7673] |   NmapOps::NmapOps();
...
            [ 7673] | main() {
  14.193  s [ 7673] |   nmap_main();
  14.193  s [ 7673] | } /* main */

...

       -D, --depth=DEPTH          Trace functions within DEPTH
       -F, --filter=FUNC          Only trace those FUNCs
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace replay -D 2
# DURATION    TID     FUNCTION
            [ 7673] | _GLOBAL__sub_I__ZN3DNS7Factory13progressiveIdE() {
   7.245 us [ 7673] |   open();
  21.938 us [ 7673] |   read();
  59.669 us [ 7673] | } /* _GLOBAL__sub_I__ZN3DNS7Factory13progressiveIdE */
   6.125 us [ 7673] | _GLOBAL__sub_I__Z16set_program_namePKc();
            [ 7673] | _GLOBAL__sub_I_o() {
   5.718 us [ 7673] |   NmapOps::NmapOps();
...
            [ 7673] | main() {
  14.193  s [ 7673] |   nmap_main();
  14.193  s [ 7673] | } /* main */

...

       -D, --depth=DEPTH          Trace functions within DEPTH
       -F, --filter=FUNC          Only trace those FUNCs
```

Not important !

```
$ uftrace replay -D 3 -F main
# DURATION    TID     FUNCTION
            [ 7673] | main() {
            [ 7673] |   nmap_main() {
  36.916 us [ 7673] |     localtime();
  15.758 us [ 7673] |     parse_options();
  48.699 us [ 7673] |     tty_init();
 143.925 ms [ 7673] |     apply_delayed_options();
  19.436 us [ 7673] |     ctime();
 106.828 us [ 7673] |     NmapOps::XSLStyleSheet();
   7.032 us [ 7673] |     xml_start_document();
   6.040 us [ 7673] |     xml_attribute();
  10.399 us [ 7673] |     xml_write_escaped();
 206.983 us [ 7673] |     output_xml_scaninfo_records();
...
```

```
        -D, --depth=DEPTH          Trace functions within DEPTH
        -F, --filter=FUNC          Only trace those FUNCs
```

Replay in 3 depth level

with example data

But too many functions..

Step 3. Statistics and summary

$ man uftrace **report**

```
NAME
       uftrace-report - Print statistics and summary for trace data

SYNOPSIS
       uftrace report [options]

DESCRIPTION
       This command collects trace data from a given data file and prints sta-
       tistics and summary information.  It shows function statistics  by  de-
       fault,  but  can  show  thread statistics with the --threads option and
       show differences between traces with the --diff option.

...
```

```
$ uftrace report
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   14.193  s   16.465 us           1  main
   14.193  s   80.617 us           1  nmap_main
   13.373  s  165.279 ms           2  ultra_scan
   13.151  s    3.474 ms        1172  do_one_select_round
   13.147  s   13.147  s         814  select
  883.098 ms    0.501 us           1  nexthost
  883.097 ms   15.743 us           1  refresh_hostbatch
  381.225 ms    0.714 us           1  nmap_mass_rdns
  381.225 ms  131.629 us           1  nmap_mass_rdns_core
  379.970 ms  379.970 ms           1  epoll_wait
  292.927 ms    2.250 us           1  TargetGroup::get_next_host
  292.925 ms   13.247 us           1  NetBlockHostname::resolve
  292.911 ms    1.278 us           1  resolve_all
  292.910 ms  292.910 ms           1  getaddrinfo
  143.925 ms   27.309 us           1  apply_delayed_options
  143.661 ms    7.293 ms           1  gettoppts
  135.620 ms   87.742 ms           1  nmap_services_init
   46.393 ms   21.499 ms           2  std::__cxx11::list::sort
   44.670 ms   18.142 ms        2002  sendConnectScanProbe
   25.039 ms   25.039 ms        2002  connect
...
```

```
$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
   13.373  s  165.279 ms           2  ultra_scan
  135.620 ms   87.742 ms           1  nmap_services_init
   25.039 ms   25.039 ms        2002  connect
   24.875 ms   24.761 ms         719  std::__cxx11::list::merge
   46.393 ms   21.499 ms           2  std::__cxx11::list::sort
   44.670 ms   18.142 ms        2002  sendConnectScanProbe
  143.661 ms    7.293 ms           1  gettoppts
    5.533 ms    5.533 ms         865  std::_Rb_tree::_M_erase
    3.727 ms    3.727 ms         318  close
   13.151  s    3.474 ms        1172  do_one_select_round
    3.099 ms    3.099 ms           1  std::__cxx11::list::~list
    5.880 ms    2.392 ms         607  HostScanStats::markProbeTimedout
    1.851 ms    1.366 ms         197  keyWasPressed
    1.346 ms    1.346 ms         196  socket
    1.260 ms    1.187 ms         145  next_token
  942.693 us  942.693 us           1  std::ios_base::ios_base
    2.117 ms  857.682 us           1  load_payloads_from_file
...
                          -s, --sort=KEY[,KEY,...]   Sort reported functions by KEYs
```

```
$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ========================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
   13.373  s  165.279 ms           2  ultra_scan
  135.620 ms   87.742 ms           1  nmap_services_init
   25.039 ms   25.039 ms        2002  connect
   24.875 ms   24.761 ms         719  std::__cxx11::list::merge
   46.393 ms   21.499 ms           2  std::__cxx11::list::sort
   44.670 ms   18.142 ms        2002  sendConnectScanProbe
  143.661 ms    7.293 ms           1  gettoppts
    5.533 ms    5.533 ms         865  std::_Rb_tree::_M_erase
    3.727 ms    3.727 ms         318  close
   13.151  s    3.474 ms        1172  do_one_select_round
    3.099 ms    3.099 ms           1  std::__cxx11::list::~list
    5.880 ms    2.392 ms         607  HostScanStats::markProbeTimedout
    1.851 ms    1.366 ms         197  keyWasPressed
    1.346 ms    1.346 ms         196  socket
    1.260 ms    1.187 ms         145  next_token
  942.693 us  942.693 us           1  std::ios_base::ios_base
    2.117 ms  857.682 us           1  load_payloads_from_file
...
                                 -s, --sort=KEY[,KEY,...]   Sort reported functions by KEYs
```

Not important !

```
$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ========================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
   13.373  s  165.279 ms           2  ultra_scan
  135.620 ms   87.742 ms           1  nmap_services_init
   25.039 ms   25.039 ms        2002  connect
   24.875 ms   24.761 ms         719  std::__cxx11::list::merge
   46.393 ms   21.499 ms           2  std::__cxx11::list::sort
   44.670 ms   18.142 ms        2002  sendConnectScanProbe
  143.661 ms    7.293 ms           1  gettoppts
    5.533 ms    5.533 ms         865  std::_Rb_tree::_M_erase
    3.727 ms    3.727 ms         318  close
   13.151  s    3.474 ms        1172  do_one_select_round
    3.099 ms    3.099 ms           1  std::__cxx11::list::~list
    5.880 ms    2.392 ms         607  HostScanStats::markProbeTimedout
    1.851 ms    1.366 ms         197  keyWasPressed
    1.346 ms    1.346 ms         196  socket
    1.260 ms    1.187 ms         145  next_token
  942.693 us  942.693 us           1  std::ios_base::ios_base
    2.117 ms  857.682 us           1  load_payloads_from_file
...
                                 -s, --sort=KEY[,KEY,...]   Sort reported functions by KEYs
```

Focus on funcs related to 'scan'

ultra_scan() first !

$ man uftrace **graph**

```
NAME
       uftrace-graph - Show function call graph

SYNOPSIS
       uftrace graph [options] []

DESCRIPTION
       This  command  shows  a function call graph for the given function in a
       uftrace record datafile.  If the function name is omitted, main is used
       by  default.   The  function  call graph contains backtrace and calling
       functions.  Each function in the output is annotated with a  hit  count
       and the total time spent running that function.

...
```

```
$ uftrace graph ultra_scan
...
calling functions
=================================
  13.373  s : (2) ultra_scan
   2.219 ms :  +-(1) init_payloads
  92.412 us :  |  +-(1) nmap_fetchfile
  90.022 us :  |  | (2) nmap_fetchfile_sub
  53.572 us :  |  |  +-(2) nmap_fetchfile_userdir_uid
  47.017 us :  |  |  | (2) getpwuid
            :  |  |  |
   8.384 us :  |  |  +-(1) readlink
...
            :  |
  21.104 us :  +-(2) UltraScanInfo::Init
   5.336 us :  | (1) GroupScanStats::GroupScanStats
            :  |
  44.155 ms :  +-(1995) sendConnectScanProbe
  24.683 ms :  |  +-(1995) connect
            :  |  |
   1.292 ms :  |  +-(189) socket
...
```

```
$ uftrace graph ultra_scan
...
calling functions
=================================
  13.373  s : (2) ultra_scan
   2.219 ms :  +-(1) init_payloads
  92.412 us :  |  +-(1) nmap_fetchfile
  90.022 us :  |  | (2) nmap_fetchfile_sub
  53.572 us :  |  |  +-(2) nmap_fetchfile_userdir_uid
  47.017 us :  |  |  | (2) getpwuid
            :  |  |  |
   8.384 us :  |  |  +-(1) readlink
...
            :  |
  21.104 us :  +-(2) UltraScanInfo::Init
   5.336 us :  | (1) GroupScanStats::GroupScanStats
            :  |
  44.155 ms :  +-(1995) sendConnectScanProbe
  24.683 ms :  |  +-(1995) connect
            :  |  |
   1.292 ms :  |  +-(189) socket
...
```

Oh, too many call counts

```
$ uftrace graph ultra_scan
...
calling functions
=====================================
  13.373  s : (2) ultra_scan
   2.219 ms :  +-(1) init_payloads
  92.412 us :  |  +-(1) nmap_fetchfile
  90.022 us :  |  | (2) nmap_fetchfile_sub
  53.572 us :  |  |  +-(2) nmap_fetchfile_userdir_uid
  47.017 us :  |  |  | (2) getpwuid
            :  |  |  |
   8.384 us :  |  |  +-(1) readlink
...
            :  |
  21.104 us :  +-(2) UltraScanInfo::Init
   5.336 us :  | (1) GroupScanStats::GroupScanStats
            :  |
  44.155 ms :  +-(1995) sendConnectScanProbe
  24.683 ms :  |  +-(1995) connect
            :  |  |
   1.292 ms :  |  +-(189) socket
...
```

Moreover nested connect(), socket()

Looking into

sendConnectScanProbe() !

```
$ cd nmap/

$ grep -n sendConnectScanProbe *.cc
scan_engine.cc:2210:    sendConnectScanProbe(USI, hss, pspec.pd.tcp.dport, 0, 0);
scan_engine.cc:2232:    sendConnectScanProbe(USI, hss, pspec.pd.tcp.dport, pspec_tries + 1, 0);
scan_engine.cc:2295:    sendConnectScanProbe(USI, hss, hss->target->pingprobe.pd.tcp.dport, 0,
scan_engine.cc:2380:    newProbe = sendConnectScanProbe(USI, hss, probe->pspec()->pd.tcp.dport, probe-
>tryno + 1, 0);
scan_engine_connect.cc:424:UltraProbe *sendConnectScanProbe(UltraScanInfo *USI, HostScanStats *hss,
```

Ah, it is function header

```
$ cd nmap/

$ grep -n sendConnectScanProbe *.cc
scan_engine.cc:2210:    sendConnectScanProbe(USI, hss, pspec.pd.tcp.dport, 0, 0);
scan_engine.cc:2232:    sendConnectScanProbe(USI, hss, pspec.pd.tcp.dport, pspec_tries + 1, 0);
scan_engine.cc:2295:    sendConnectScanProbe(USI, hss, hss->target->pingprobe.pd.tcp.dport, 0,
scan_engine.cc:2380:    newProbe = sendConnectScanProbe(USI, hss, probe->pspec()->pd.tcp.dport, probe-
>tryno + 1, 0);
scan_engine_connect.cc:424:UltraProbe *sendConnectScanProbe(UltraScanInfo *USI, HostScanStats *hss,


$ emacs scan_engine_connect.cc
...
422 /* If this is NOT a ping probe, set pingseq to 0.  Otherwise it will be the
423    ping sequence number (they start at 1).  The probe sent is returned. */
424 UltraProbe *sendConnectScanProbe(UltraScanInfo *USI, HostScanStats *hss,
425                                   u16 destport, u8 tryno, u8 pingseq) {
...
```

Oh, is it **port number** ?

Step 4. Print Arguments

```
424 UltraProbe *sendConnectScanProbe(UltraScanInfo *USI, HostScanStats *hss,
425                                  u16 destport, u8 tryno, u8 pingseq) {
...

$ cd ../ && cd uftrace.data.nmap_args/
$ uftrace replay -F sendConnectScanProbe -D 1 -A sendConnectScanProbe@arg3

# DURATION    TID     FUNCTION
  87.474 us [31689] | sendConnectScanProbe(80);
  34.240 us [31689] | sendConnectScanProbe(443);
  75.963 us [31689] | sendConnectScanProbe(1723);
  35.326 us [31689] | sendConnectScanProbe(199);
  20.016 us [31689] | sendConnectScanProbe(25);
  17.195 us [31689] | sendConnectScanProbe(113);
  20.688 us [31689] | sendConnectScanProbe(143);
  17.541 us [31689] | sendConnectScanProbe(3306);
  16.678 us [31689] | sendConnectScanProbe(53);
  16.493 us [31689] | sendConnectScanProbe(22);
  15.893 us [31689] | sendConnectScanProbe(111);
...
```

```
424 UltraProbe *sendConnectScanProbe(UltraScanInfo *USI, HostScanStats *hss,
425                                  u16 destport, u8 tryno, u8 pingseq) {
...

$ cd ../ && cd uftrace.data.nmap_args/
$ uftrace replay -F sendConnectScanProbe -D 1 -A sendConnectScanProbe@arg3

# DURATION    TID     FUNCTION
  87.474 us [31689] | sendConnectScanProbe(80);
  34.240 us [31689] | sendConnectScanProbe(443);
  75.963 us [31689] | sendConnectScanProbe(1723);
  35.326 us [31689] | sendConnectScanProbe(199);
  20.016 us [31689] | sendConnectScanProbe(25);
  17.195 us [31689] | sendConnectScanProbe(113);
  20.688 us [31689] | sendConnectScanProbe(143);
  17.541 us [31689] | sendConnectScanProbe(3306);
  16.678 us [31689] | sendConnectScanProbe(53);
  16.493 us [31689] | sendConnectScanProbe(22);
  15.893 us [31689] | sendConnectScanProbe(111);
...
```

```
424 UltraProbe *sendConnectScanProbe(UltraScanInfo *USI, HostScanStats *hss,
425                                  u16 destport, u8 tryno, u8 pingseq) {
...

$ cd ../ && cd uftrace.data.nmap_args/
$ uftrace replay -F sendConnectScanProbe -D 1 -A sendConnectScanProbe@arg3

# DURATION    TID     FUNCTION
  87.474 us [31689] | sendConnectScanProbe(80);
  34.240 us [31689] | sendConnectScanProbe(443);
  75.963 us [31689] | sendConnectScanProbe(1723);
  35.326 us [31689] | sendConnectScanProbe(199);
  20.016 us [31689] | sendConnectScanProbe(25);
  17.195 us [31689] | sendConnectScanProbe(113);
  20.688 us [31689] | sendConnectScanProbe(143);
  17.541 us [31689] | sendConnectScanProbe(3306);
  16.678 us [31689] | sendConnectScanProbe(53);
  16.493 us [31689] | sendConnectScanProbe(22);
  15.893 us [31689] | sendConnectScanProbe(111);
...
```

http

ssh

```
424 UltraProbe *sendConnectScanProbe(UltraScanInfo *USI, HostScanStats *hss,
425                                  u16 destport, u8 tryno, u8 pingseq) {
...

$ cd ../ && cd uftrace.data.nmap_args/
$ uftrace replay -F sendConnectScanProbe -D 1 -A sendConnectScanProbe@arg3

# DURATION    TID     FUNCTION
  87.474 us [31689] | sendConnectScanProbe(80);
  34.240 us [31689] | sendConnectScanProbe(443);
  75.963 us [31689] | sendConnectScanProbe(1723);
  35.326 us [31689] | sendConnectScanProbe(199);
  20.016 us [31689] | sendConnectScanProbe(25);
  17.195 us [31689] | sendConnectScanProbe(113);
  20.688 us [31689] | sendConnectScanProbe(143);
  17.541 us [31689] | sendConnectScanProbe(3306);
  16.678 us [31689] | sendConnectScanProbe(53);
  16.493 us [31689] | sendConnectScanProbe(22);
  15.893 us [31689] | sendConnectScanProbe(111);
...
```

This is a port scan sequence

Nmap scans well-known port numbers first

Event Tracing (sched event)

-E linux:schedule

```
$ uftrace t-fork
# DURATION    TID     FUNCTION
   1.609 us [32272] | __monstartup();
   1.493 us [32272] | __cxa_atexit();
            [32272] | main() {
 189.898 us [32272] |   fork();
            [32272] |   wait() {

            [32275] |   } /* fork */
            [32275] |   a() {
            [32275] |     b() {
            [32275] |       c() {
   3.899 us [32275] |         getpid();
   5.974 us [32275] |       } /* c */
   6.690 us [32275] |     } /* b */
   7.437 us [32275] |   } /* a */
  16.142 us [32275] | } /* main */

 956.108 us [32272] |   } /* wait */
            [32272] |   a() {
            [32272] |     b() {
            [32272] |       c() {
   4.290 us [32272] |         getpid();
   5.868 us [32272] |       } /* c */
   6.515 us [32272] |     } /* b */
   7.132 us [32272] |   } /* a */
   1.177 ms [32272] | } /* main */
```

Multiprocess program example

```
$ uftrace -E linux:schedule t-fork
# DURATION    TID     FUNCTION
   1.609 us [32272] | __monstartup();
   1.493 us [32272] | __cxa_atexit();
            [32272] | main() {
 189.898 us [32272] |   fork();
            [32272] |   wait() {
            [32272] |     /* linux:sched-out */
            [32275] |   } /* fork */
            [32275] |   a() {
            [32275] |     b() {
            [32275] |       c() {
   3.899 us [32275] |         getpid();
   5.974 us [32275] |       } /* c */
   6.690 us [32275] |     } /* b */
   7.437 us [32275] |   } /* a */
  16.142 us [32275] | } /* main */
 919.404 us [32272] |     /* linux:sched-in */
 956.108 us [32272] |   } /* wait */
            [32272] |   a() {
            [32272] |     b() {
            [32272] |       c() {
   4.290 us [32272] |         getpid();
   5.868 us [32272] |       } /* c */
   6.515 us [32272] |     } /* b */
   7.132 us [32272] |   } /* a */
   1.177 ms [32272] | } /* main */
```

You can see the scheduling event

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
...
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
...
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
...
```

Due to waiting time..

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
...
# uftrace record -E linux:schedule -d uftrace.data.nmap_sched -- ./nmap nmap.org
$ cd ../ && cd uftrace.data.nmap_sched/
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
...
# uftrace record -E linux:schedule -d uftrace.data.nmap_sched -- ./nmap nmap.org
$ cd ../ && cd uftrace.data.nmap_sched/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   12.048  s   12.048  s         108  linux:schedule
   11.884  s  150.189 ms           2  ultra_scan
  140.047 ms   87.156 ms           1  nmap_services_init
...
   11.673  s    8.548 ms         597  select
...
```

It excludes schedule-out time

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -d uftrace.data.nmap_nmap.org -- ./nmap nmap.org
$ cd uftrace.data.nmap_nmap.org/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   13.147  s   13.147  s         814  select
  379.970 ms  379.970 ms           1  epoll_wait
  292.910 ms  292.910 ms           1  getaddrinfo
...
# uftrace record -E linux:schedule -d uftrace.data.nmap_sched -- ./nmap nmap.org
$ cd ../ && cd uftrace.data.nmap_sched/

$ uftrace report -s self
  Total time   Self time       Calls  Function
  ==========  ==========  ==========  ====================================
   12.048  s   12.048  s         108  linux:schedule
   11.884  s  150.189 ms           2  ultra_scan
  140.047 ms   87.156 ms           1  nmap_services_init
...
   11.673  s    8.548 ms         597  select
...
```

Due to waiting time..

It excludes schedule-out time

User + Kernel Tracing

Nmap example

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -K 3 -d uftrace.data.nmap_kern -- ./nmap nmap.org
$ cd uftrace.data.nmap_kern/
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -K 3 -d uftrace.data.nmap_kern -- ./nmap nmap.org
$ cd uftrace.data.nmap_kern/

$ uftrace graph sendIPScanProbe
  78.812 ms : (2003) sendIPScanProbe
  66.874 ms :  +-(2003) send_ip_packet
  64.529 ms :  |  +-(2003) sendto
  60.876 ms :  |  |  +-(2003) sys_sendto
   2.706 ms :  |  |  |  +-(2003) sockfd_lookup_light
   1.010 ms :  |  |  |  |  +-(2003) __fdget
            :  |  |  |  |  |
  49.669 us :  |  |  |  |  +-(1) smp_apic_timer_interrupt
            :  |  |  |  |
 915.096 us :  |  |  |  +-(2003) move_addr_to_kernel.part.14
            :  |  |  |  |
  51.020 ms :  |  |  |  +-(2003) sock_sendmsg
   1.732 ms :  |  |  |  |  +-(2003) security_socket_sendmsg
  22.254 us :  |  |  |  |  | (1) smp_apic_timer_interrupt
            :  |  |  |  |  |
  41.848 ms :  |  |  |  |  +-(2003) inet_sendmsg
  20.826 us :  |  |  |  |  | (1) smp_apic_timer_interrupt
            :  |  |  |  |  |
  64.012 us :  |  |  |  |  +-(3) smp_apic_timer_interrupt
            :  |  |  |  |  |
  14.037 us :  |  |  |  |  +-(2) do_IRQ
...
```

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -K 3 -d uftrace.data.nmap_kern -- ./nmap nmap.org
$ cd uftrace.data.nmap_kern/

$ uftrace graph sendIPScanProbe
  78.812 ms : (2003) sendIPScanProbe
  66.874 ms :  +-(2003) send_ip_packet
  64.529 ms :  |  +-(2003) sendto
  60.876 ms :  |  |  +-(2003) sys_sendto
   2.706 ms :  |  |  |  +-(2003) sockfd_lookup_light
   1.010 ms :  |  |  |  |  +-(2003) __fdget
            :  |  |  |  |  |
  49.669 us :  |  |  |  |  +-(1) smp_apic_timer_interrupt
            :  |  |  |  |
 915.096 us :  |  |  |  +-(2003) move_addr_to_kernel.part.14
            :  |  |  |  |
  51.020 ms :  |  |  |  +-(2003) sock_sendmsg
   1.732 ms :  |  |  |  |  +-(2003) security_socket_sendmsg
  22.254 us :  |  |  |  |  | (1) smp_apic_timer_interrupt
            :  |  |  |  |  |
  41.848 ms :  |  |  |  |  +-(2003) inet_sendmsg
  20.826 us :  |  |  |  |  | (1) smp_apic_timer_interrupt
            :  |  |  |  |  |
  64.012 us :  |  |  |  |  +-(3) smp_apic_timer_interrupt
            :  |  |  |  |  |
  14.037 us :  |  |  |  |  +-(2) do_IRQ
...
```

User space

```
$ cd uftrace-osseu17/nmap_examples/

# uftrace record -K 3 -d uftrace.data.nmap_kern -- ./nmap nmap.org
$ cd uftrace.data.nmap_kern/

$ uftrace graph sendIPScanProbe
  78.812 ms : (2003) sendIPScanProbe
  66.874 ms :  +-(2003) send_ip_packet
  64.529 ms :  |  +-(2003) sendto
  60.876 ms :  |  |  +-(2003) sys_sendto
   2.706 ms :  |  |  |  +-(2003) sockfd_lookup_light
   1.010 ms :  |  |  |  |  +-(2003) __fdget
            :  |  |  |  |  |
  49.669 us :  |  |  |  |  +-(1) smp_apic_timer_interrupt
            :  |  |  |  |
 915.096 us :  |  |  |  +-(2003) move_addr_to_kernel.part.14
            :  |  |  |  |
  51.020 ms :  |  |  |  +-(2003) sock_sendmsg
   1.732 ms :  |  |  |  |  +-(2003) security_socket_sendmsg
  22.254 us :  |  |  |  |  | (1) smp_apic_timer_interrupt
            :  |  |  |  |  |
  41.848 ms :  |  |  |  |  +-(2003) inet_sendmsg
  20.826 us :  |  |  |  |  | (1) smp_apic_timer_interrupt
            :  |  |  |  |  |
  64.012 us :  |  |  |  |  +-(3) smp_apic_timer_interrupt
            :  |  |  |  |  |
  14.037 us :  |  |  |  |  +-(2) do_IRQ
...
```

User space

Kernel space

User + Kernel Tracing

printf() example

(x86_64, xen)

```
$ cd uftrace-osseu17/printf_kern_examples/

$ cd uftrace.data.printf_kern/
```

```
$ cd uftrace-osseu17/printf_kern_examples/

$ cd uftrace.data.printf_kern/
```

recorded data on X86_64

```
$ cd uftrace-osseu17/printf_kern_examples/

$ cd uftrace.data.printf_kern/
```

recorded data on X86_64

```
$ uftrace replay
# DURATION    TID     FUNCTION
   1.057 us [31071] | __monstartup();
   0.940 us [31071] | __cxa_atexit();
            [31071] | main() {
            [31071] |   printf() {
...
            [31071] |     sys_write() {
            [31071] |       __fdget_pos() {
   0.470 us [31071] |         __fget_light();
   1.337 us [31071] |       } /* __fdget_pos */
            [31071] |       vfs_write() {
            [31071] |         rw_verify_area() {
   1.224 us [31071] |           security_file_permission();
   2.330 us [31071] |         } /* rw_verify_area */
            [31071] |         __vfs_write() {
  13.830 us [31071] |           tty_write();
```

```
$ cd uftrace-osseu17/printf_kern_examples/

$ cd uftrace.data.printf_xen/
```

```
$ cd uftrace-osseu17/printf_kern_examples/

$ cd uftrace.data.printf_xen/
```

recorded data on xen

```
$ cd uftrace-osseu17/printf_kern_examples/

$ cd uftrace.data.printf_xen/
```

recorded data on xen

```
$ uftrace replay
# DURATION    TID     FUNCTION
   3.215 us [ 3148] | __monstartup();
   2.751 us [ 3148] | __cxa_atexit();
            [ 3148] | main() {
            [ 3148] |   printf() {
...
            [ 3148] |     sys_write() {
            [ 3148] |       xen_evtchn_do_upcall() {
            [ 3148] |         irq_enter() {
   0.423 us [ 3148] |           rcu_irq_enter();
   2.085 us [ 3148] |         } /* irq_enter */
...
            [ 3148] |           tty_write() {
   1.842 us [ 3148] |             xen_evtchn_do_upcall();
   1.050 us [ 3148] |             xen_maybe_preempt_hcall();
  25.477 us [ 3148] |           } /* tty_write */
...
```

User + Kernel Tracing

Process Lifecycle

fork() → exec() → main() → exit() → schedule()

```
$ cd uftrace-osseu17/process_life_cycle_example/

# uftrace record -K 5 ./hello
$ cd uftrace.data
```

```
$ cd uftrace-osseu17/process_life_cycle_example/

# uftrace record -K 5 ./hello
$ cd uftrace.data

$ uftrace replay --kernel-full
# DURATION    TID     FUNCTION
   3.817 us [ 1037] | finish_task_switch();
   0.434 us [ 1037] | _raw_spin_lock_irq();
   0.375 us [ 1037] | __fsnotify_parent();
   0.335 us [ 1037] | fsnotify();
            [ 1037] | sys_execve() {
...
            [ 1037] | main() {
            [ 1037] |   printf() {
...
            [ 1037] |     sys_write() {
...
  20.088 us [ 1037] |     } /* sys_write */
  39.679 us [ 1037] |   } /* printf */
   1.166 us [ 1037] |   fflush();
  41.453 us [ 1037] | } /* main */
...
            [ 1037] | sys_exit_group() {
            [ 1037] |   do_group_exit() {          --kernel-full Show kernel functions outside of user
...
            [ 1037] |       schedule() {
   0.386 us [ 1037] |         rcu_note_context_switch();
```

```
$ cd uftrace-osseu17/process_life_cycle_example/

# uftrace record -K 5 ./hello
$ cd uftrace.data

$ uftrace replay --kernel-full
# DURATION    TID     FUNCTION
   3.817 us [ 1037] | finish_task_switch();
   0.434 us [ 1037] | _raw_spin_lock_irq();
   0.375 us [ 1037] | __fsnotify_parent();
   0.335 us [ 1037] | fsnotify();
            [ 1037] | sys_execve() {
...
            [ 1037] | main() {
            [ 1037] |   printf() {
...
            [ 1037] |     sys_write() {
...
  20.088 us [ 1037] |     } /* sys_write */
  39.679 us [ 1037] |   } /* printf */
   1.166 us [ 1037] |   fflush();
  41.453 us [ 1037] | } /* main */
...
            [ 1037] | sys_exit_group() {
            [ 1037] |   do_group_exit() {          --kernel-full Show kernel functions outside of user
...
            [ 1037] |       schedule() {
   0.386 us [ 1037] |         rcu_note_context_switch();
```

```
$ cd uftrace-osseu17/process_life_cycle_example/

# uftrace record -K 5 ./hello
$ cd uftrace.data

$ uftrace replay --kernel-full
# DURATION    TID     FUNCTION
   3.817 us [ 1037] | finish_task_switch();
   0.434 us [ 1037] | _raw_spin_lock_irq();
   0.375 us [ 1037] | __fsnotify_parent();
   0.335 us [ 1037] | fsnotify();
            [ 1037] | sys_execve() {
...
            [ 1037] | main() {
            [ 1037] |   printf() {
...
            [ 1037] |     sys_write() {
...
  20.088 us [ 1037] |     } /* sys_write */
  39.679 us [ 1037] |   } /* printf */
   1.166 us [ 1037] |   fflush();
  41.453 us [ 1037] | } /* main */
...
            [ 1037] | sys_exit_group() {
            [ 1037] |   do_group_exit() {
...
            [ 1037] |       schedule() {
   0.386 us [ 1037] |         rcu_note_context_switch();
```

fork()

exec()

main()

exit()

schedule()

It shows process life cycle

Production quality programs examples

with --chrome option

(V8, clang and perf)

```
$ cd uftrace-osseu17/chrome_tracing_examples

$ ls
clang_internal.json        v8_CPU_intensive.json
perf_record_internal.json  v8_mem_intensive.json

$ google-chrome

        --chrome   Dump recorded data in chrome trace format
```

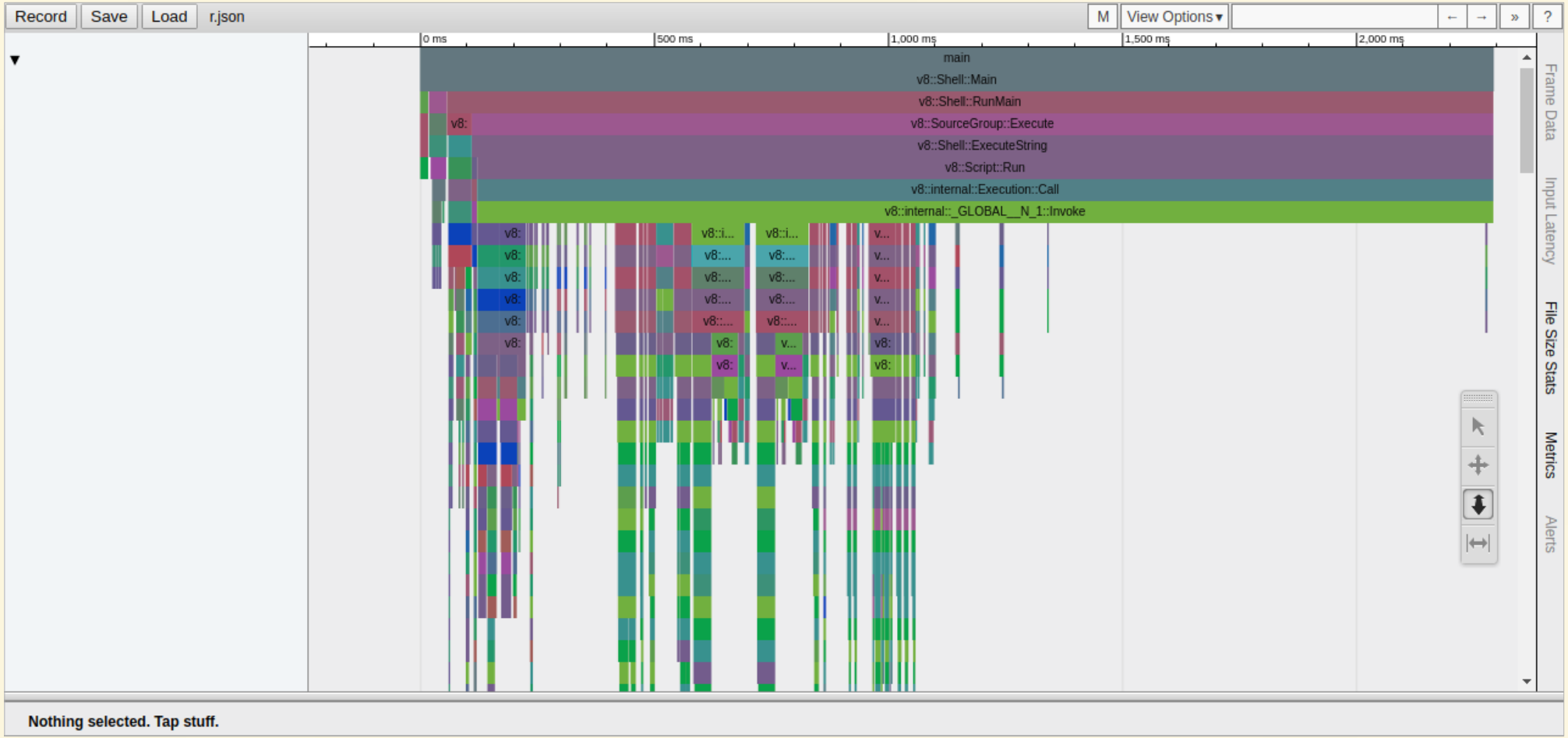
Run chrome browser

and

Load .json file

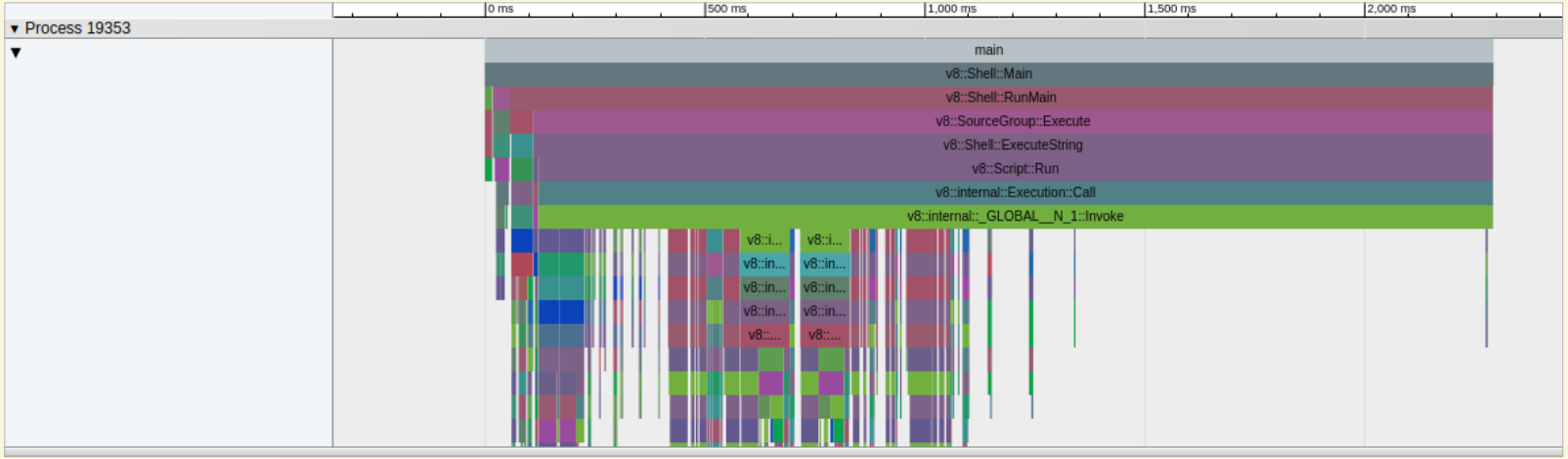
on chrome://tracing

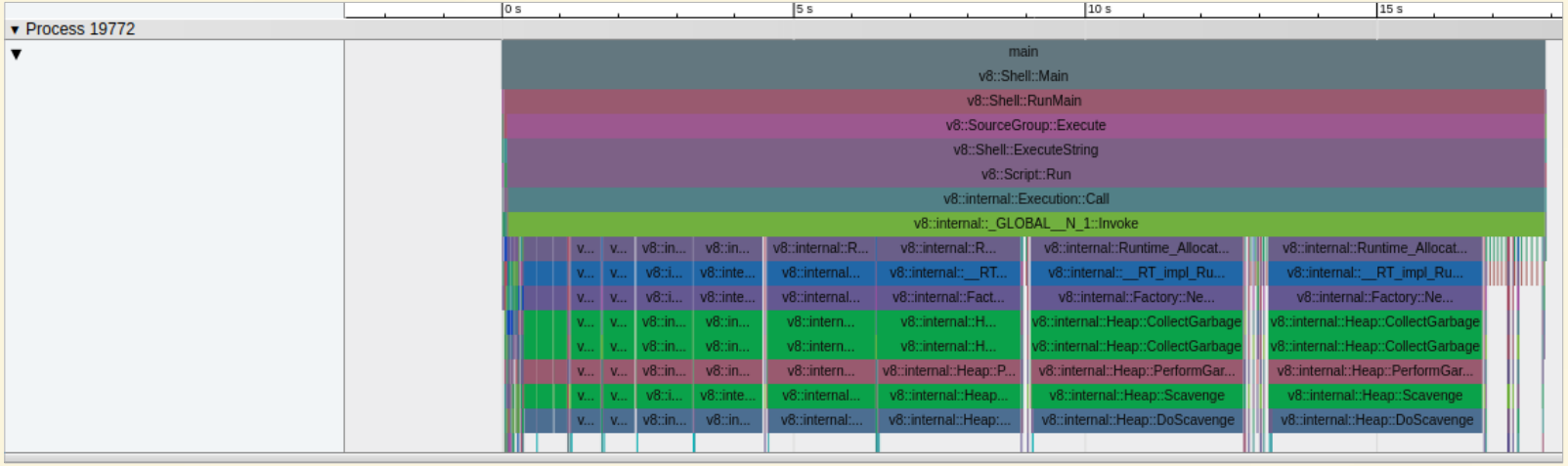
You can zoom in-out on chrome://tracing



What is different between

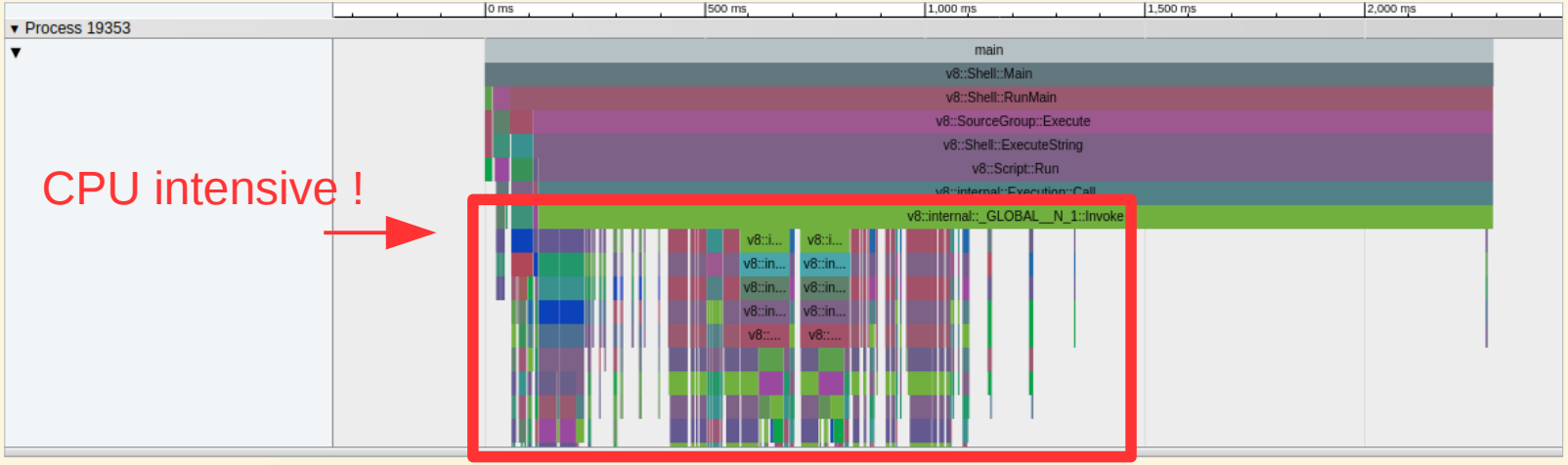
v8_CPU_intensive.json and v8_mem_intensive.json ?

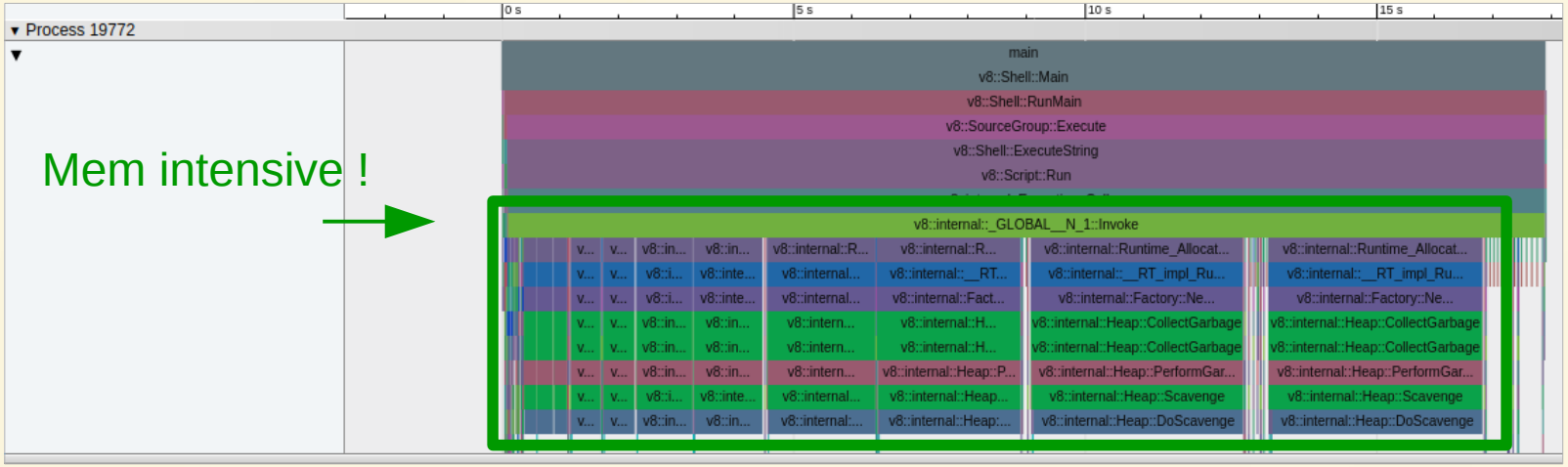




What is different between

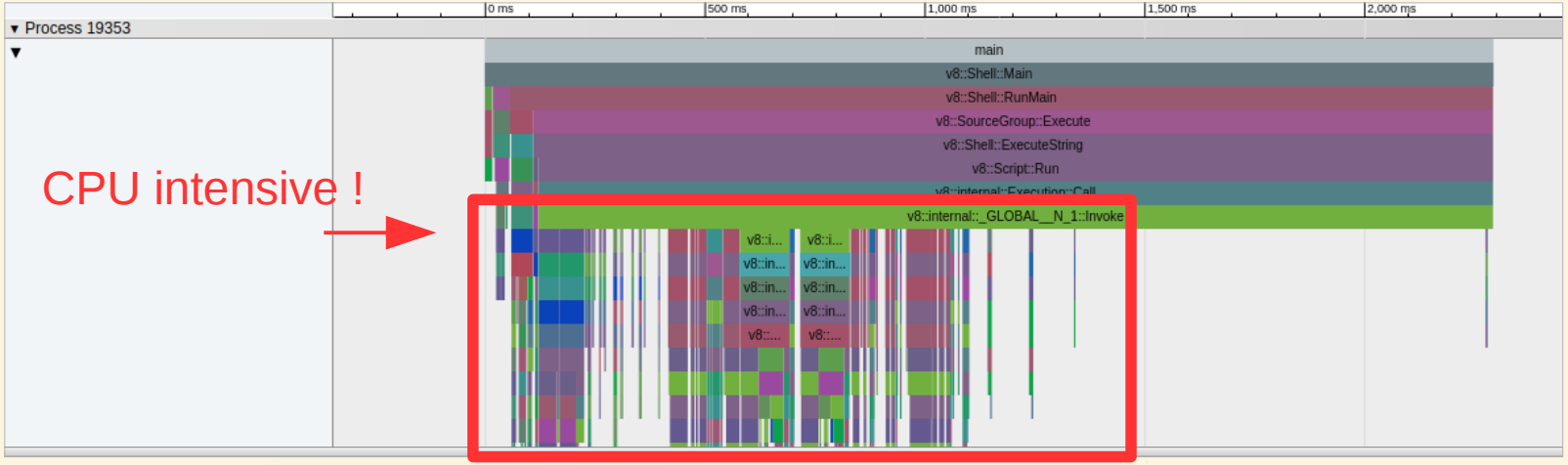
v8_CPU_intensive.json and v8_mem_intensive.json ?

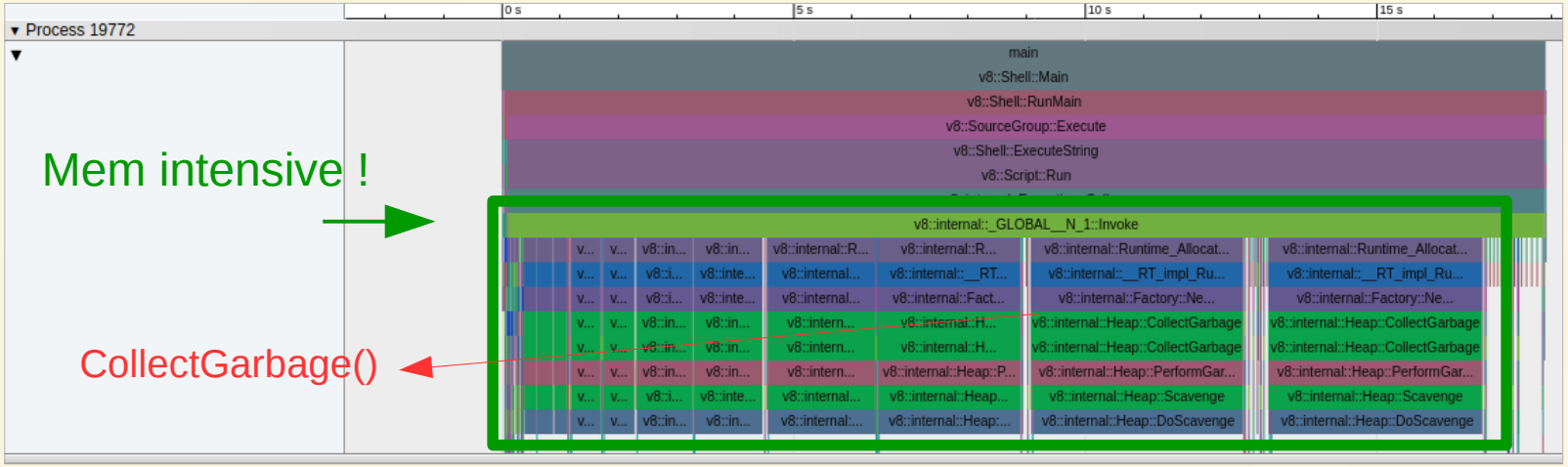




What is different between

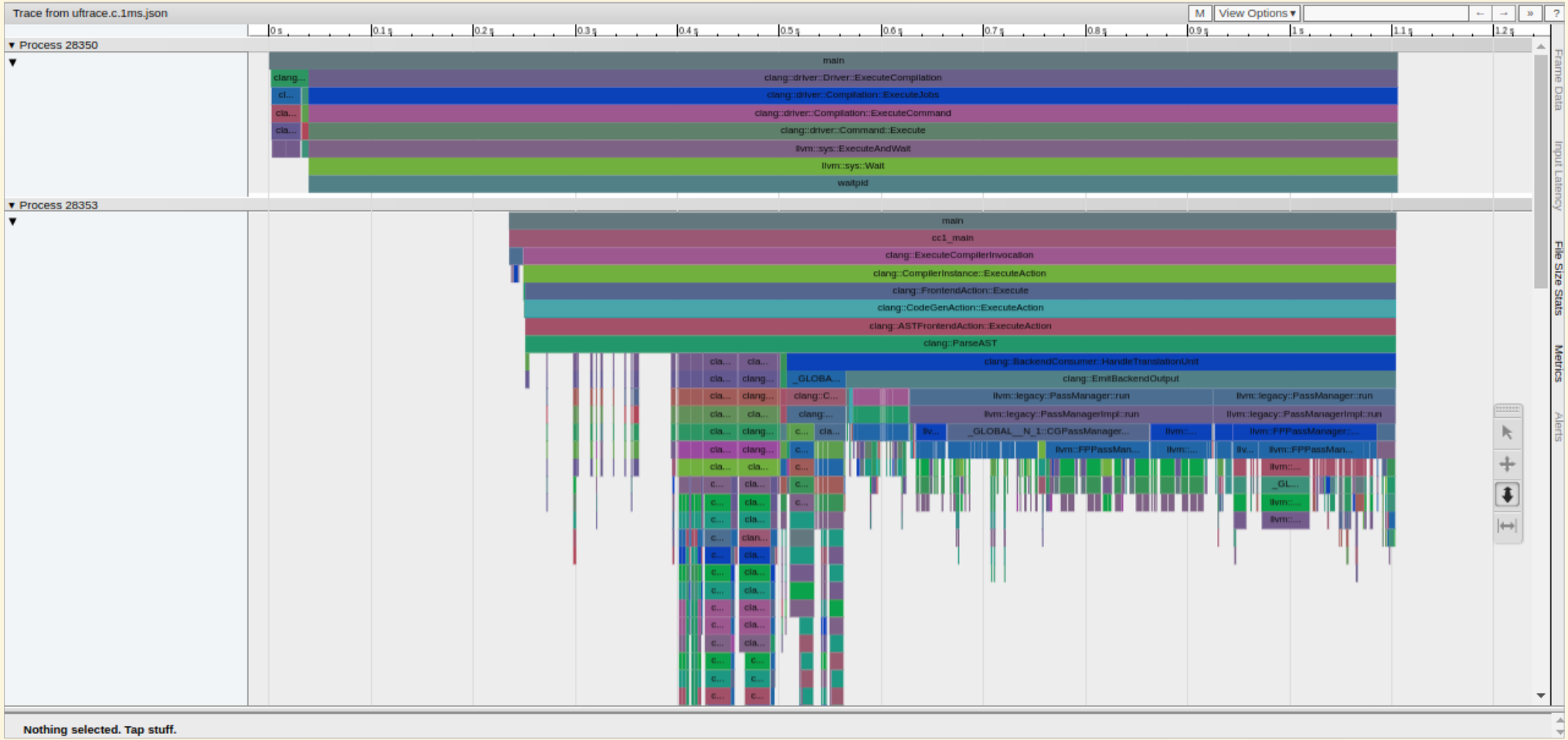
v8_CPU_intensive.json and v8_mem_intensive.json ?





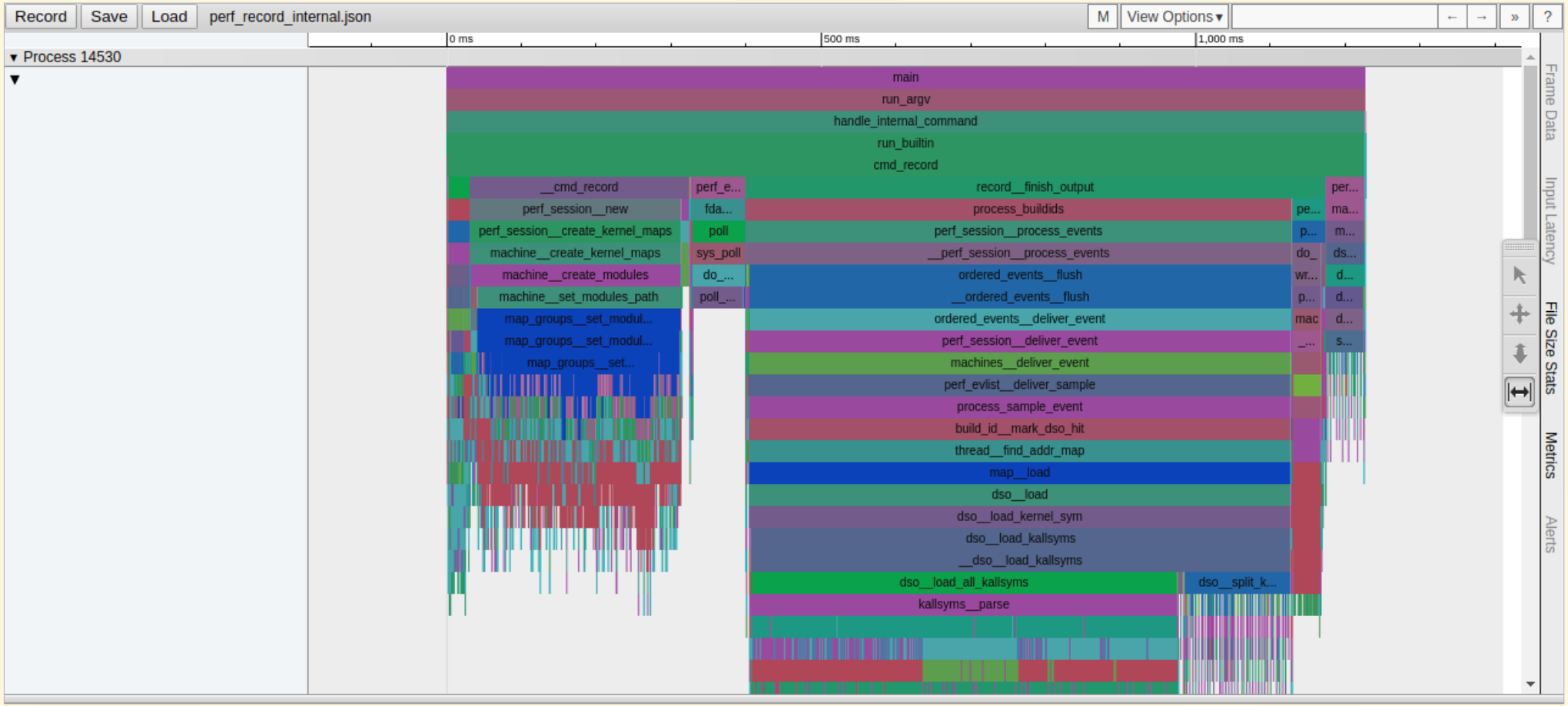
clang_internal.json → chrome://tracing

(A trace of clang (LLVM) compiling uftrace src)



perf_internal.json → chrome://tracing

(A trace of perf profiling uftrace)



Python interpreter tracing

.py VS. **.pyc**

```
$ cd uftrace-osseu17/cpython_example

$ cd uftrace.data.hello_py && uftrace graph
calling functions
=====================================
 101.647 ms : (1) main
 101.563 ms : (1) Py_Main
  85.513 ms :  +-(1) Py_Initialize
  85.513 ms :  | (1) _Py_InitializeEx_Private.part.8
   6.298 ms :  |  +-(1) _Py_ReadyTypes
            :  |  |
   1.368 ms :  |  +-(1) _PyExc_Init
            :  |  |
   1.425 ms :  |  +-(1) _PySys_Init
            :  |  |
  16.101 ms :  |  +-(1) import_init
   2.894 ms :  |  |  +-(1) PyImport_ImportFrozenModule
   2.892 ms :  |  |  | (1) PyImport_ImportFrozenModuleObject
   1.273 ms :  |  |  |  +-(1) PyMarshal_ReadObjectFromString
   1.271 ms :  |  |  |  | (1) r_object
   1.238 ms :  |  |  |  | (1) r_object
            :  |  |  |  |
   1.585 ms :  |  |  |  +-(1) PyEval_EvalCode
   1.584 ms :  |  |  |    (1) _PyEval_EvalCodeWithName
   1.581 ms :  |  |  |    (1) _PyEval_EvalFrameDefault
            :  |  |  |
  12.220 ms :  |  |  +-(1) PyObject_CallMethod
  12.215 ms :  |  |    (1) PyObject_Call
  12.215 ms :  |  |    (1) function_call
  12.215 ms :  |  |    (1) PyEval_EvalCodeEx
...
```

recorded data
'python hello.py'

A trace of python running .py

```
$ cd .. & cd uftrace.data.hello_pyc

$ uftrace graph
calling functions
=====================================
  95.862 ms : (1) main
  95.778 ms : (1) Py_Main
  81.528 ms :  +-(1) Py_Initialize
  81.528 ms :  | (1) _Py_InitializeEx_Private.part.8
   6.309 ms :  |  +-(1) _Py_ReadyTypes
           :  |  |
   1.329 ms :  |  +-(1) _PyExc_Init
           :  |  |
   1.461 ms :  |  +-(1) _PySys_Init
           :  |  |
  15.573 ms :  |  +-(1) import_init
   2.889 ms :  |  |  +-(1) PyImport_ImportFrozenModule
   2.888 ms :  |  |  | (1) PyImport_ImportFrozenModuleObject
   1.268 ms :  |  |  |  +-(1) PyMarshal_ReadObjectFromString
   1.266 ms :  |  |  |  | (1) r_object
   1.233 ms :  |  |  |  | (1) r_object
           :  |  |  |  |
   1.585 ms :  |  |  |  +-(1) PyEval_EvalCode
   1.584 ms :  |  |  |    (1) _PyEval_EvalCodeWithName
   1.581 ms :  |  |  |    (1) _PyEval_EvalFrameDefault
           :  |  |  |
  12.034 ms :  |  |  +-(1) PyObject_CallMethod
  12.029 ms :  |  |    (1) PyObject_Call
  12.029 ms :  |  |    (1) function_call
  12.029 ms :  |  |    (1) PyEval_EvalCodeEx
...
```

recorded data
'python hello.pyc'

Check call graph of cpython running .pyc

```
$ uftrace report --diff-policy=percent -d uftrace.data.hello_py --diff uftrace.data.hello_pyc
#
# uftrace diff
#  [0] base: uftrace.data.hello_py      (from uftrace record -t 1ms -d uftrace.data.hello_py ./python hello.py )
#  [1] diff: uftrace.data.hello_pyc     (from uftrace record -t 1ms -d uftrace.data.hello_pyc ./python __pycache__/hello.cpython-
36.pyc )
#
                 Total time (diff)                  Self time (diff)                      Calls (diff)   Function
  ================================   ================================   ================================   ==========================
   12.005 ms    9.328 ms   -22.30%    29.956 us   19.007 us   -36.55%           1          1          0   _PyCodecRegistry_Init
   11.975 ms    9.309 ms   -22.26%     1.551 us    1.044 us   -32.69%           1          1          0   PyImport_ImportModuleNoBlock
   13.531 ms   11.039 ms   -18.41%     7.693 us    6.273 us   -18.46%           1          1          0   initfsencoding.isra.5
   13.523 ms   11.033 ms   -18.41%     4.264 us    4.986 us   +16.93%           1          1          0   _PyCodec_Lookup
    6.556 ms    5.668 ms   -13.55%    14.558 us   12.911 us   -11.31%           4          4          0   marshal_loads
    1.513 ms    1.700 ms   +12.32%     0.139 us    0.130 us    -6.47%           1          1          0   PyEval_CallObjectWithKeywords
   10.436 ms    9.508 ms    -8.89%     1.203 ms    1.066 ms   -11.36%           1          1          0   PyImport_Cleanup
    9.232 ms    8.441 ms    -8.56%     1.575 us    1.007 us   -36.06%           2          2          0   _PyGC_CollectNoFail
    9.520 ms    8.735 ms    -8.24%     9.520 ms    8.735 ms    -8.24%          14         14          0   r_object
   15.142 ms   13.948 ms    -7.88%   312.846 us  237.433 us   -24.11%           1          1          0   Py_FinalizeEx.part.3
   15.142 ms   13.948 ms    -7.88%     0.322 us    0.307 us    -4.66%           1          1          0   Py_FinalizeEx
    2.541 ms    2.344 ms    -7.76%     2.541 ms    2.344 ms    -7.76%           1          1          0   PyInit_posix
   13.623 ms   12.642 ms    -7.20%    13.623 ms   12.642 ms    -7.20%           3          3          0   collect
   56.833 ms   53.235 ms    -6.33%    45.423 us   38.517 us   -15.20%           4          4          0   PyImport_Import
   56.787 ms   53.196 ms    -6.32%     6.530 us    6.232 us    -4.56%           4          4          0   PyObject_CallFunction
    1.710 ms    1.817 ms    +6.30%     1.020 us    1.441 us   +41.27%           1          1          0   _imp_get_frozen_object
   58.193 ms   54.778 ms    -5.87%    20.930 us   18.956 us    -9.43%           7          7          0   builtin___import__
   63.565 ms   59.863 ms    -5.82%    18.856 us    8.682 us   -16.65%          16         17         +1   PyCFunction_Call
  101.563 ms   95.778 ms    -5.70%   907.452 us  301.311 us   -66.80%           1          1          0   Py_Main
  101.647 ms   95.862 ms    -5.69%    83.999 us   84.121 us    +0.15%           1          1          0   main
   11.886 ms   11.209 ms    -5.69%     9.094 us    8.175 us   -10.11%           7          7          0   _PyCFunction_FastCallKeywords
   70.315 ms   66.710 ms    -5.13%   357.353 us  297.186 us   -16.84%          90         89         -1   _PyFunction_FastCall
   69.878 ms   66.297 ms    -5.12%    38.914 us   27.980 us   -28.10%         100        100          0   call_function
   70.510 ms   66.920 ms    -5.09%     2.002 us    1.945 us    -2.85%           6          6          0   PyObject_Call
   72.052 ms   68.449 ms    -5.00%    57.987 ms   55.468 ms    -4.34%         123        124         +1   _PyEval_EvalFrameDefault
   62.573 ms   59.486 ms    -4.93%    25.997 us   23.394 us   -10.01%          18         18          0   _PyObject_CallMethodIdObjArgs
   62.563 ms   59.476 ms    -4.93%     2.505 us    2.462 us    -1.72%          18         18          0   _PyObject_FastCallDict
   62.562 ms   59.475 ms    -4.93%     2.921 us    3.039 us    +4.04%          18         18          0   _PyFunction_FastCallDict
...
                                                                          --diff=DATA            Report differences
                                                                          --diff-policy=POLICY   Control diff report policy
```

Optimization Level Comparison

-O1 / -O2 / -O3

```
$ cd uftrace-osseu17/optimization_level_examples

$ cd uftrace.data.knap_O1/ && uftrace replay
# DURATION    TID     FUNCTION
   2.180 us [ 5863] | __monstartup();
   2.651 us [ 5863] | __cxa_atexit();
            [ 5863] | main() {
  19.250 us [ 5863] |   fgets();
            [ 5863] |   get_values_from() {
   4.090 us [ 5863] |     __strdup();
   3.082 us [ 5863] |     strchr();
   3.268 us [ 5863] |     strtol();
   0.767 us [ 5863] |     strtol();
  14.764 us [ 5863] |   } /* get_values_from */
   7.246 us [ 5863] |   malloc();
   0.947 us [ 5863] |   fgets();
            [ 5863] |   get_values_from() {
   1.007 us [ 5863] |     __strdup();
   0.617 us [ 5863] |     strtol();
   4.586 us [ 5863] |   } /* get_values_from */
   0.546 us [ 5863] |   fgets();
            [ 5863] |   get_values_from() {
   0.661 us [ 5863] |     __strdup();
   0.501 us [ 5863] |     strtol();
   3.644 us [ 5863] |   } /* get_values_from */
            [ 5863] |   get_values_from() {
   0.697 us [ 5863] |     __strdup();
   0.531 us [ 5863] |     strtol();
   0.517 us [ 5863] |     strtol();
   4.030 us [ 5863] |   } /* get_values_from */
   0.567 us [ 5863] |   fgets();
...
```

Too many

Repeated func calls

```
$ uftrace graph
calling functions
=====================================
 306.501 ms : (1) main
  63.685 us :  +-(46) fgets
            :  |
   1.747 ms :  +-(941) get_values_from
  78.848 us :  |  +-(72) __strdup
            :  |  |
   3.082 us :  |  +-(1) strchr
            :  |  |
  27.050 us :  |  +-(46) strtol
            :  |
   9.912 us :  +-(2) malloc
            :  |
 303.826 ms :  +-(940) pack_knapsack
   1.445 ms :  | (182) get_cond_maxprice
            :  |
  14.071 us :  +-(1) printf
            :  |
   1.353 us :  +-(1) free

...
```

So, change view

uftrace graph

```
$ uftrace graph
calling functions
=====================================
 306.501 ms : (1) main
  63.685 us :  +-(46) fgets
            :  |
   1.747 ms :  +-(941) get_values_from
  78.848 us :  |  +-(72) __strdup
            :  |  |
   3.082 us :  |  +-(1) strchr
            :  |  |
  27.050 us :  |  +-(46) strtol
            :  |
   9.912 us :  +-(2) malloc
            :  |
 303.826 ms :  +-(940) pack_knapsack
   1.445 ms :  | (182) get_cond_maxprice
            :  |
  14.071 us :  +-(1) printf
            :  |
   1.353 us :  +-(1) free

...
```

-O1

-O2

```
$ cd ../ && uftrace.data.knap_O2

$ uftrace graph
calling functions
=====================================
  15.019 ms : (1) main
  13.344 us :  +-(3) fgets
            :  |
   1.166 ms :  +-(941) get_values_from
  26.613 us :  |  +-(12) __strdup
            :  |  |
   1.493 us :  |  +-(1) strchr
            :  |  |
   1.570 us :  |  +-(1) strtol
            :  |
   6.408 us :  +-(2) malloc
            :  |
  13.242 ms :  +-(940) pack_knapsack
            :  |
  16.331 us :  +-(1) printf
            :  |
   1.641 us :  +-(1) free


...
```

get_cond_maxprice() **inlined**

-O1

-O2

```
$ uftrace report -d uftrace.data.knap_O1 --diff uftrace.data.knap_O2
#
# uftrace diff
#  [0] base: uftrace.data.knap_O1      (from uftrace record -t 0.5us -d uftrace.data.knap_O1 knapsack_O1 )
#  [1] diff: uftrace.data.knap_O2      (from uftrace record -t 0.5us -d uftrace.data.knap_O2 knapsack_O2 )
#
                    Total time (diff)                     Self time (diff)                      Calls (diff)   Function
  ===================================   ===================================   ================================   =================
  306.501 ms   15.019 ms  -291.481 ms   838.433 us  573.861 us  -264.572 us            1          1          0   main
  303.826 ms   13.242 ms  -290.584 ms   302.381 ms   13.242 ms  -289.139 ms          940        940          0   pack_knapsack
    1.445 ms           -    -1.445 ms     1.445 ms           -    -1.445 ms          182          0       -182   get_cond_maxprice
    1.747 ms    1.166 ms  -581.066 us     1.638 ms    1.136 ms  -501.762 us          941        941          0   get_values_from
   78.848 us   26.613 us   -52.235 us    78.848 us   26.613 us   -52.235 us           72         12        -60   __strdup
   63.685 us   13.344 us   -50.341 us    63.685 us   13.344 us   -50.341 us           46          3        -43   fgets
   27.050 us    1.570 us   -25.480 us    27.050 us    1.570 us   -25.480 us           46          1        -45   strtol
    9.912 us    6.408 us    -3.504 us     9.912 us    6.408 us    -3.504 us            2          2          0   malloc
   14.071 us   16.331 us    +2.260 us    14.071 us   16.331 us    +2.260 us            1          1          0   printf
    3.082 us    1.493 us    -1.589 us     3.082 us    1.493 us    -1.589 us            1          1          0   strchr
    2.651 us    1.189 us    -1.462 us     2.651 us    1.189 us    -1.462 us            1          1          0   __cxa_atexit
    2.180 us    1.115 us    -1.065 us     2.180 us    1.115 us    -1.065 us            1          1          0   __monstartup
    1.353 us    1.641 us    +0.288 us     1.353 us    1.641 us    +0.288 us            1          1          0   free

...
                                                                  --diff=DATA            Report differences
                                                                  --diff-policy=POLICY   Control diff report policy
```

```
$ cd ../ && uftrace.data.knap_O2

$ uftrace graph
calling functions
=====================================
  15.019 ms : (1) main
  13.344 us :  +-(3) fgets
            :  |
   1.166 ms :  +-(941) get_values_from
  26.613 us :  |  +-(12) __strdup
            :  |  |
   1.493 us :  |  +-(1) strchr
            :  |  |
   1.570 us :  |  +-(1) strtol
            :  |
   6.408 us :  +-(2) malloc
            :  |
  13.242 ms :  +-(940) pack_knapsack
            :  |
  16.331 us :  +-(1) printf
            :  |
   1.641 us :  +-(1) free


...
```

O2

```
$ cd ../ && uftrace.data.knap_O2

$ uftrace graph
calling functions
=====================================
  15.019 ms : (1) main
  13.344 us :  +-(3) fgets
            :  |
   1.166 ms :  +-(941) get_values_from
  26.613 us :  |  +-(12) __strdup
            :  |  |
   1.493 us :  |  +-(1) strchr
            :  |  |
   1.570 us :  |  +-(1) strtol
            :  |
   6.408 us :  +-(2) malloc
            :  |
  13.242 ms :  +-(940) pack_knapsack
            :  |
  16.331 us :  +-(1) printf
            :  |
   1.641 us :  +-(1) free


...
```

O2

O3

```
$ cd ../ && uftrace.data.knap_O3

$ uftrace graph
calling functions
=====================================
   7.143 ms : (1) main
   8.452 us :  +-(3) fgets
            :  |
   3.917 us :  +-(1) get_values_from
   1.060 us :  |  +-(1) __strdup
            :  |  |
   0.760 us :  |  +-(1) strchr
            :  |  |
   0.896 us :  |  +-(1) strtol
            :  |
   3.249 us :  +-(2) malloc
            :  |
   9.401 us :  +-(7) __strdup
            :  |
  11.063 us :  +-(1) memset
            :  |
  11.866 us :  +-(1) printf
            :  |
   1.370 us :  +-(1) free

...
```

Reduced call counts
941 → 1

pack_knapsack()
inlined into main()

O2

O3

```
$ uftrace report -d uftrace.data.knap_O2 --diff uftrace.data.knap_O3
#
# uftrace diff
#  [0] base: uftrace.data.knap_O2      (from uftrace record -t 0.5us -d uftrace.data.knap_O2 knapsack_O2 )
#  [1] diff: uftrace.data.knap_O3      (from uftrace record -t 0.5us -d uftrace.data.knap_O3 knapsack_O3 )
#
                    Total time (diff)                     Self time (diff)                      Calls (diff)   Function
  ===================================   ===================================   ================================   =================
   13.242 ms           -   -13.242 ms    13.242 ms           -   -13.242 ms          940          0       -940   pack_knapsack
   15.019 ms    7.143 ms    -7.875 ms   573.861 us    7.094 ms    +6.520 ms            1          1          0   main
    1.166 ms    3.917 us    -1.162 ms     1.136 ms    1.201 us    -1.135 ms          941          1       -940   get_values_from
   26.613 us   10.461 us   -16.152 us    26.613 us   10.461 us   -16.152 us           12          8         -4   __strdup
           -   11.063 us   +11.063 us            -   11.063 us   +11.063 us            0          1         +1   memset
   13.344 us    8.452 us    -4.892 us    13.344 us    8.452 us    -4.892 us            3          3          0   fgets
   16.331 us   11.866 us    -4.465 us    16.331 us   11.866 us    -4.465 us            1          1          0   printf
    6.408 us    3.249 us    -3.159 us     6.408 us    3.249 us    -3.159 us            2          2          0   malloc
    1.493 us    0.760 us    -0.733 us     1.493 us    0.760 us    -0.733 us            1          1          0   strchr
    1.570 us    0.896 us    -0.674 us     1.570 us    0.896 us    -0.674 us            1          1          0   strtol
    1.189 us    0.709 us    -0.480 us     1.189 us    0.709 us    -0.480 us            1          1          0   __cxa_atexit
    1.115 us    0.663 us    -0.452 us     1.115 us    0.663 us    -0.452 us            1          1          0   __monstartup
    1.641 us    1.370 us    -0.271 us     1.641 us    1.370 us    -0.271 us            1          1          0   free

...
                                                                                --diff=DATA            Report differences
                                                                                --diff-policy=POLICY   Control diff report policy
```

NULL Pointer Exception case

GDB core VS. uftrace.data

```
$ cd uftrace-osseu17/nullptr_exception_example

$ ./benchmark_STL_containers_nullptr
*** Error in `./benchmark_STL_containers_nullptr': double free or
corruption (fasttop): 0x0000000002389710 ***
======= Backtrace: =========
/lib/x86_64-linux-gnu/libc.so.6(+0x777e5)[0x7f29349ae7e5]
/lib/x86_64-linux-gnu/libc.so.6(+0x8037a)[0x7f29349b737a]
/lib/x86_64-linux-gnu/libc.so.6(cfree+0x4c)[0x7f29349bb53c]
./benchmark_STL_containers_nullptr[0x400c8a]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf0)[0x7f2934957830]
./benchmark_STL_containers_nullptr[0x400ea9]
======= Memory map: ========
...
Aborted (core dumped)
```

Crash case

If some program crash,

core file contains the last stacktrace

```
$ gdb ./benchmark_STL_containers_nullptr core
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
...
Reading symbols from ./benchmark_STL_containers_nullptr...(no debugging symbols found)...done.

warning: core file may not match specified executable file.
[New LWP 15820]
Core was generated by `./benchmark_STL_containers_nullptr'.
Program terminated with signal SIGABRT, Aborted.
#0  0x00007f607e166428 in __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:54
54   ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  0x00007f607e166428 in __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:54
#1  0x00007f607e16802a in __GI_abort () at abort.c:89
#2  0x00007f607e1a87ea in __libc_message (do_abort=do_abort@entry=2, fmt=fmt@entr=0x7f607e2c1e98 ...
#3  0x00007f607e1b137a in malloc_printerr (ar_ptr=<optimized out>, ptr=<optimized out>,..
#4  _int_free (av=<optimized out>, p=<optimized out>, have_lock=0) at malloc.c:3867
#5  0x00007f607e1b553c in __GI___libc_free (mem=<optimized out>) at malloc.c:2968
#6  0x0000000000400c8a in main ()
(gdb)
```

uftrace contains full trace

until the crash point

```
# cd uftrace.data.nullptr/ && uftrace replay
$ uftrace ./benchmark_STL_containers_nullptr
```

```
# cd uftrace.data.nullptr/ && uftrace replay
$ uftrace ./benchmark_STL_containers_nullptr
*** Error in `./benchmark_STL_containers_nullptr': double free or corruption (fasttop): ...
...
process crashed by signal 6: Aborted (si_code: -6)
child terminated by signal: 6: Aborted
# DURATION    TID     FUNCTION
            [30869] | main() {
            [30869] |   bench_vector_push_back() {
   0.842 us [30869] |     std::vector::_M_insert_aux();
   3.036 us [30869] |     std::vector::_M_insert_aux();
   1.246 us [30869] |     std::vector::_M_insert_aux();
   1.648 us [30869] |     std::vector::_M_insert_aux();
  10.665 us [30869] |   } /* bench_vector_push_back */
   2.153 us [30869] |   bench_deque_push_back();
            [30869] |   bench_list_push_back() {
...
  11.736 us [30869] |   } /* bench_list_push_back */
   0.139 us [30869] |   operator new();
   0.168 us [30869] |   operator delete();
   0.110 us [30869] |   operator delete();
            [30869] |   operator delete() {

uftrace stopped tracing with remaining functions
================================================
task: 3651
[1] operator delete
[0] main
```

```
# cd uftrace.data.nullptr/ && uftrace replay
$ uftrace ./benchmark_STL_containers_nullptr
*** Error in `./benchmark_STL_containers_nullptr': double free or corruption (fasttop): ...
...
process crashed by signal 6: Aborted (si_code: -6)
child terminated by signal: 6: Aborted
# DURATION    TID     FUNCTION
            [30869] | main() {
            [30869] |   bench_vector_push_back() {
   0.842 us [30869] |     std::vector::_M_insert_aux();
   3.036 us [30869] |     std::vector::_M_insert_aux();
   1.246 us [30869] |     std::vector::_M_insert_aux();
   1.648 us [30869] |     std::vector::_M_insert_aux();
  10.665 us [30869] |   } /* bench_vector_push_back */
   2.153 us [30869] |   bench_deque_push_back();
            [30869] |   bench_list_push_back() {
...
  11.736 us [30869] |   } /* bench_list_push_back */
   0.139 us [30869] |   operator new();
   0.168 us [30869] |   operator delete();
   0.110 us [30869] |   operator delete();
            [30869] |   operator delete() {

uftrace stopped tracing with remaining functions
=========================================
task: 3651
[1] operator delete
[0] main
```

Crash point !

```
# cd uftrace.data.nullptr/ && uftrace replay
$ uftrace ./benchmark_STL_containers_nullptr
*** Error in `./benchmark_STL_containers_nullptr': double free or corruption (fasttop): ...
...
process crashed by signal 6: Aborted (si_code: -6)
child terminated by signal: 6: Aborted
# DURATION    TID     FUNCTION
            [30869] | main() {
            [30869] |   bench_vector_push_back() {
   0.842 us [30869] |     std::vector::_M_insert_aux();
   3.036 us [30869] |     std::vector::_M_insert_aux();
   1.246 us [30869] |     std::vector::_M_insert_aux();
   1.648 us [30869] |     std::vector::_M_insert_aux();
  10.665 us [30869] |   } /* bench_vector_push_back */
   2.153 us [30869] |   bench_deque_push_back();
            [30869] |   bench_list_push_back() {
...
  11.736 us [30869] |   } /* bench_list_push_back */
   0.139 us [30869] |   operator new();
   0.168 us [30869] |   operator delete();
   0.110 us [30869] |   operator delete();
            [30869] |   operator delete() {

uftrace stopped tracing with remaining functions
=========================================================
task: 3651
[1] operator delete
[0] main
```

Full trace
untill the Crash point

Crash point !

Dynamic Tracing

-pg built binary calls mcount()

at the entry of each function

uftrace preloads its mcount()

instead of mcount() in libc.so

uftrace preloads its mcount()

instead of mcount() in libc.so

LD_PRELOAD=libmcount.so

```
$ gcc -pg -o fibonacci tests/s-fibonacci.c

$ readelf -s fibonacci | grep mcount
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND mcount@GLIBC_2.2.5 (2)
    63: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND mcount@@GLIBC_2.2.5
```

You can check mcont() !

```
$ gcc -pg -o fibonacci tests/s-fibonacci.c

$ readelf -s fibonacci | grep mcount
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND mcount@GLIBC_2.2.5 (2)
    63: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND mcount@@GLIBC_2.2.5

$ objdump -d fibonacci

    <fib>:
           push   %rbp
           mov    %rsp,%rbp
           call  <mcount@plt>

    <main>:
           push   %rbp
           mov    %rsp,%rbp
           call  <mcount@plt>
```

You can check mcont() !

Performance issue ?

Dynamic Tracing

- compile time: mcount() → NOP
- runtime : NOP → trace function (e.g. mcount, fentry)

```
$ gcc -pg -mfentry -o fibonacci \
> tests/s-fibonacci.c
```

mcount()

→ **__fentry__()**

```
$ gcc -pg -mfentry -o fibonacci \
> tests/s-fibonacci.c

$ objdump -d fibonacci

    <fib>:
          call  <__fentry__@plt>
          push   %rbp
          mov    %rsp,%rbp

    <main>:
          call  <__fentry__@plt>
          push   %rbp
          mov    %rsp,%rbp
```

mcount()

→ **__fentry__()**

at the very beginning

```
$ gcc -pg -mfentry -mnop-mcount -o fibonacci \
> tests/s-fibonacci.c

$ objdump -d fibonacci

    <fib>:
          nop
          push   %rbp
          mov    %rsp,%rbp

    <main>:
          nop
          push   %rbp
          mov    %rsp,%rbp
```

__fentry__()

→ **nop**

at the very beginning

```
$ man uftrace record


-P FUNC, --patch=FUNC
        Patch FUNC dynamically.  This is only applicable
        binaries built with  -pg -mfentry -mnop-mcount  on
        x86_64.  This option can be used more than once.
        See DYNAMIC TRACING.
```

Dynamic Tracing

```
$ uftrace fibonacci 5
ERROR: Can't find 'mcount' symbol in the 'fibonacci'.


    <fib>:
            nop
            push   %rbp
            mov    %rsp,%rbp


    <main>:
            nop
            push   %rbp
            mov    %rsp,%rbp
```

Normal Tracing

Error !

Because of No mcount()

```
$ uftrace -P fib fibonacci 5


    <fib>:
           call  <__fentry__@plt>
           push   %rbp
           mov    %rsp,%rbp


    <main>:
           nop
           push   %rbp
           mov    %rsp,%rbp


 -P, --patch=FUNC   Apply dynamic patching for FUNCs
```

Dynamic Tracing

nop → __fentry__()

```
$ uftrace -P fib fibonacci 5
# DURATION    TID     FUNCTION
   0.639 us [18039] | __monstartup();
   0.481 us [18039] | __cxa_atexit();
            [18039] | fib() {
            [18039] |   fib() {
            [18039] |     fib() {
   0.076 us [18039] |       fib();
   0.059 us [18039] |       fib();
   0.546 us [18039] |     } /* fib */
   0.042 us [18039] |     fib();
   0.830 us [18039] |   } /* fib */
            [18039] |   fib() {
   0.059 us [18039] |     fib();
   0.045 us [18039] |     fib();
   0.367 us [18039] |   } /* fib */
   1.447 us [18039] | } /* fib */
```

```
 -P, --patch=FUNC   Apply dynamic patching for FUNCs
```

Dynamic Tracing

nop → __fentry__()

```
$ uftrace -P . fibonacci 5
# DURATION    TID     FUNCTION
   0.610 us [17960] | __monstartup();
   0.487 us [17960] | __cxa_atexit();
            [17960] | main() {
            [17960] |   fib() {
            [17960] |     fib() {
            [17960] |       fib() {
   0.074 us [17960] |         fib();
   0.055 us [17960] |         fib();
   0.492 us [17960] |       } /* fib */
   0.059 us [17960] |       fib();
   0.765 us [17960] |     } /* fib */
            [17960] |     fib() {
   0.045 us [17960] |       fib();
   0.042 us [17960] |       fib();
   0.332 us [17960] |     } /* fib */
   1.293 us [17960] |   } /* fib */
   2.384 us [17960] | } /* main */


 -P, --patch=FUNC   Apply dynamic patching for FUNCs
```

You can dynamic trace

all functions with '-P .'

Use case

Qt QML engine bugfix using uftrace

Blog: ***https://www.kdab.com/fixing-bugs-via-lateral-thinking/***

Youtube: ***https://www.youtube.com/watch?v=lbCaBqhnckQ***

Fixing bugs via lateral thinking

21.12.2016 Giuseppe D'Angelo No comments

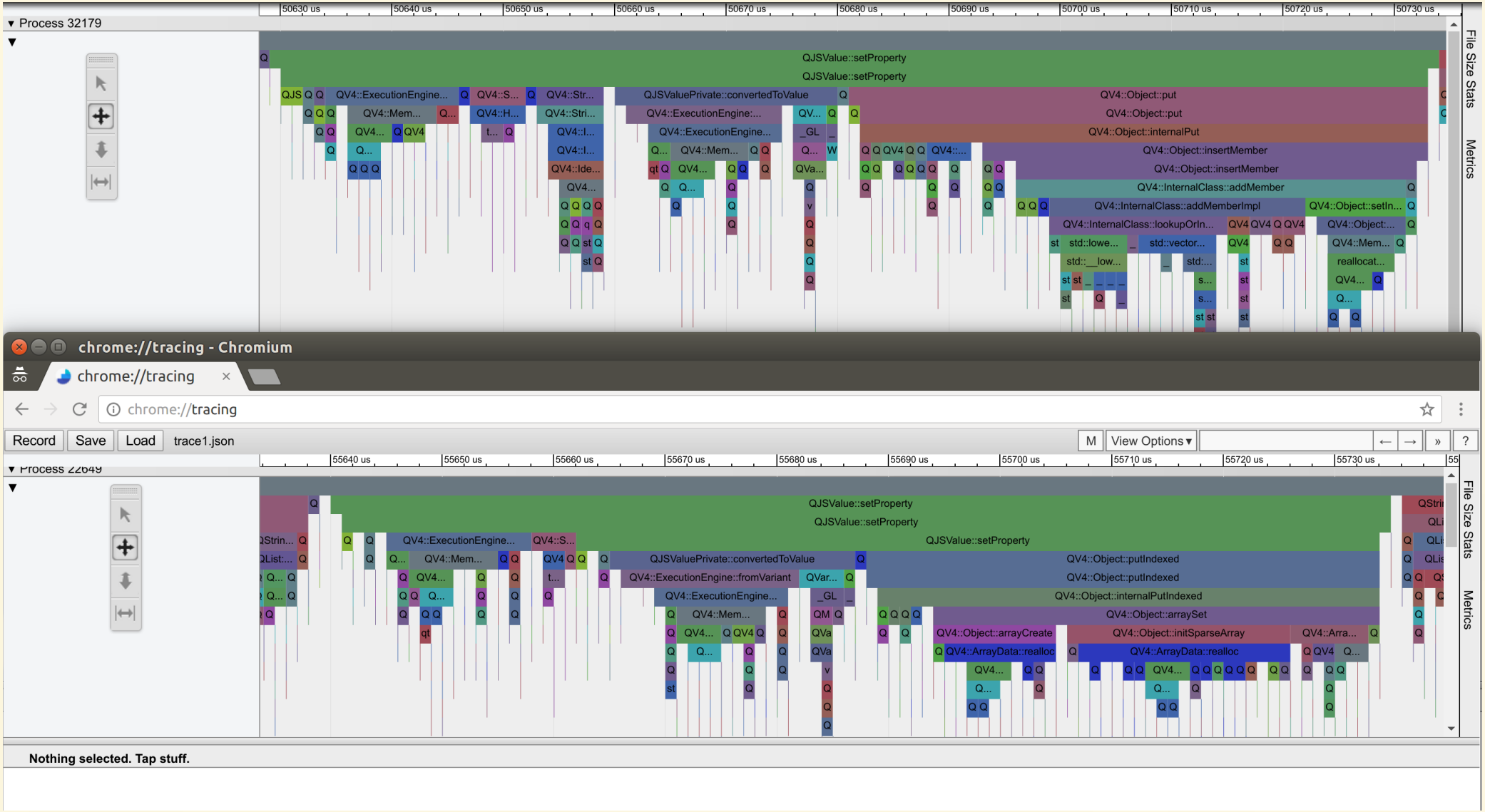
For today's blog I would like to share with you the little adventure I had when fixing a very strange bug in Qt.

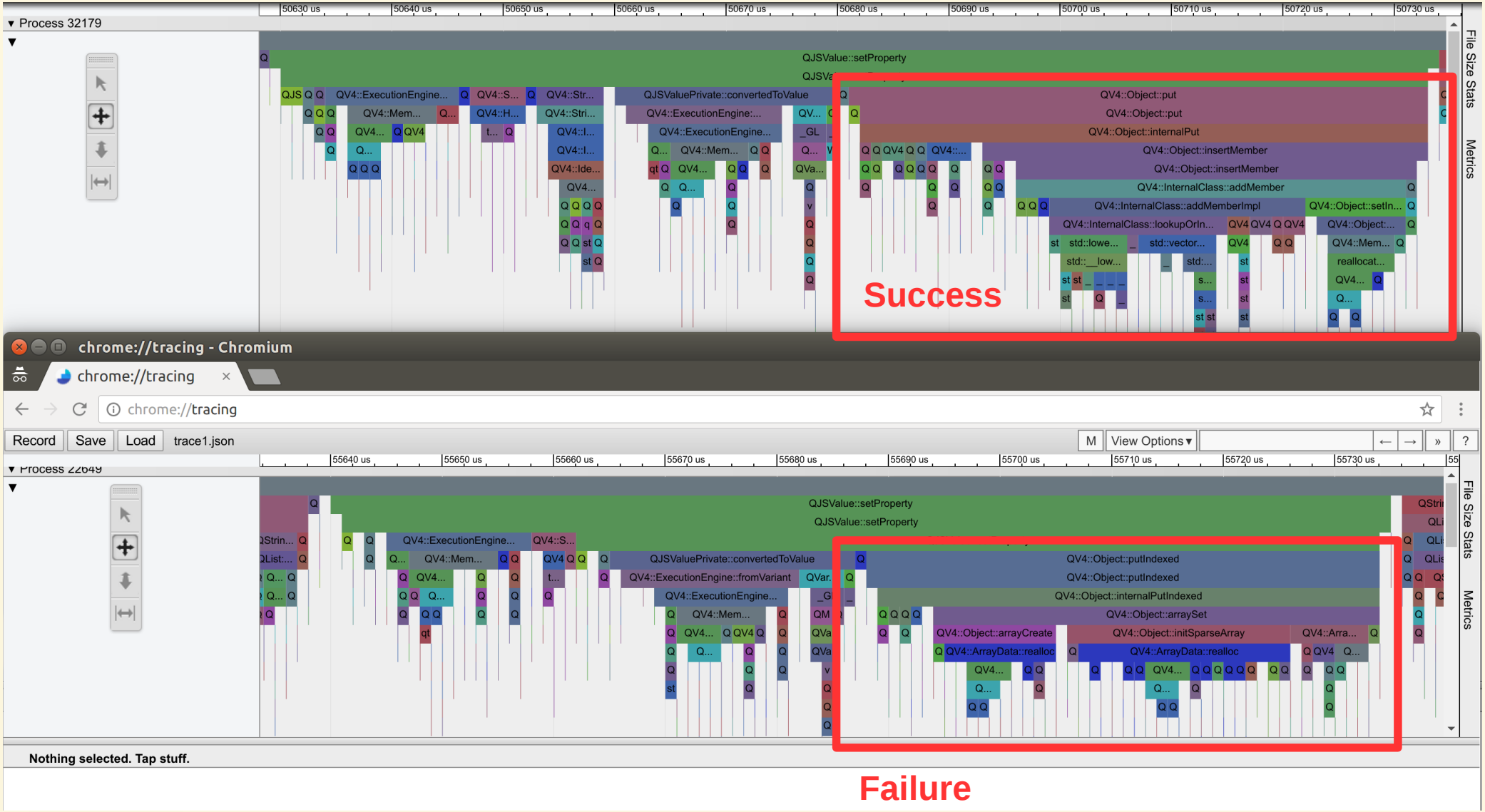
Pop quiz

Don't think about this too much, just guess: what does this QML snippet print?

```
import QtQuick 2.0

QtObject {
    Component.onCompleted: {
        console.log("240000000000" == "3776798720");
    }
}
```

There are no JavaScript semantic tricks involved; and using either `==` or `===` does not change the result in any way.


Process 32179
50630 us
50640 us
50650 us
50660 us
50670 us
50680 us
50690 us
50700 us
50710 us
50720 us
50730 us
QJSValue::setProperty
QJSValue::setProperty
QV4::ExecutionEngine...
QV4::S...
QV4::Str...
QJSValuePrivate::convertedToValue
QV4::Object::put
QV4::Object::put
QV4::Mem...
QV4::H...
QV4::Stri...
QV4::ExecutionEngine:...
QV4::ExecutionEngine...
QV4::Object::internalPut
QV4::I...
QV4::I...
QV4::Ide...
QV4::Mem...
QV4::Object::insertMember
QV4::Object::insertMember
QV4::InternalClass::addMember
QV4::InternalClass::addMemberImpl
QV4::Object::setIn...
QV4::InternalClass::lookupOrIn...
QV4::Object:...
std::lowe...
std::vector...
QV4::Mem...
std::__low...
reallocat...
File Size Stats
Metrics
chrome://tracing - Chromium
chrome://tracing
chrome://tracing
Record
Save
Load
trace1.json
M
View Options
?
Process 22649
55640 us
55650 us
55660 us
55670 us
55680 us
55690 us
55700 us
55710 us
55720 us
55730 us
QJSValue::setProperty
QJSValue::setProperty
QJSValue::setProperty
QV4::ExecutionEngine...
QV4::S...
QJSValuePrivate::convertedToValue
QV4::Object::putIndexed
QV4::Object::putIndexed
QV4::ExecutionEngine::fromVariant
QV4::ExecutionEngine...
QV4::Object::internalPutIndexed
QV4::Mem...
QV4::Object::arraySet
QV4::Object::arrayCreate
QV4::Object::initSparseArray
QV4::ArrayData::realloc
QV4::ArrayData::realloc
File Size Stats
Metrics
Nothing selected. Tap stuff.


Process 32179
QJSValue::setProperty
QV4::Object::put
QV4::Object::internalPut
QV4::Object::insertMember
QV4::InternalClass::addMember
QV4::InternalClass::addMemberImpl
QV4::InternalClass::lookupOrIn...
QJSValuePrivate::convertedToValue
QV4::ExecutionEngine::...
QV4::ExecutionEngine...
Success
File Size Stats
Metrics
chrome://tracing - Chromium
chrome://tracing
Record
Save
Load
trace1.json
M
View Options
Process 22649
QJSValue::setProperty
QV4::Object::putIndexed
QV4::Object::internalPutIndexed
QV4::Object::arraySet
QV4::Object::arrayCreate
QV4::Object::initSparseArray
QV4::ArrayData::realloc
QJSValuePrivate::convertedToValue
QV4::ExecutionEngine::fromVariant
Nothing selected. Tap stuff.
Failure

bacadi opensource project:

Node.js C++ binding code improvement using uftrace

Slide: ***https://www.slideshare.net/deview/131chromium-binging-nodejs/108***

PR: ***https://github.com/lunchclass/bacardi/pull/108***

uftrace를 사용한 call-graph 추적

DEVIEW 2017

zino — romandev@romandev-high-cpu: ~/bacardi — ssh romandev@165.227.3.183 — 80×24

```
                [ 2079] |            Napi::Value::IsNumber() {
  0.113 us      [ 2079] |              Napi::Value::Type();
  0.299 us      [ 2079] |            } /* Napi::Value::IsNumber */
                [ 2079] |            Napi::Value::ToNumber() {
                [ 2079] |              Napi::Number::Number() {
  0.060 us      [ 2079] |                Napi::Value::Value();
  0.217 us      [ 2079] |              } /* Napi::Number::Number */
  0.437 us      [ 2079] |            } /* Napi::Value::ToNumber */
  1.126 us      [ 2079] |            Napi::Number::DoubleValue();
  2.579 us      [ 2079] |          } /* NativeTypeTraits::NativeValue */
                [ 2079] |          Napi::CallbackInfo::operator [](){
  0.064 us      [ 2079] |            Napi::Value::Value();
  0.216 us      [ 2079] |          } /* Napi::CallbackInfo::operator [] */
                [ 2079] |          Napi::CallbackInfo::Env() {
  0.065 us      [ 2079] |            Napi::Env::Env();
  0.205 us      [ 2079] |          } /* Napi::CallbackInfo::Env */
                [ 2079] |          NativeTypeTraits::NativeValue() {
                [ 2079] |            Napi::Value::IsNumber() {
  0.079 us      [ 2079] |              Napi::Value::Type();
  0.245 us      [ 2079] |            } /* Napi::Value::IsNumber */
                [ 2079] |            Napi::Value::ToNumber() {
                [ 2079] |              Napi::Number::Number() {
  0.063 us      [ 2079] |                Napi::Value::Value();
:
```

Native Type Converting을 위해 Type Checking을 반복적으로 하고 있음을 알 수 있음.

https://www.slideshare.net/deview/131chromium-binging-nodejs/110

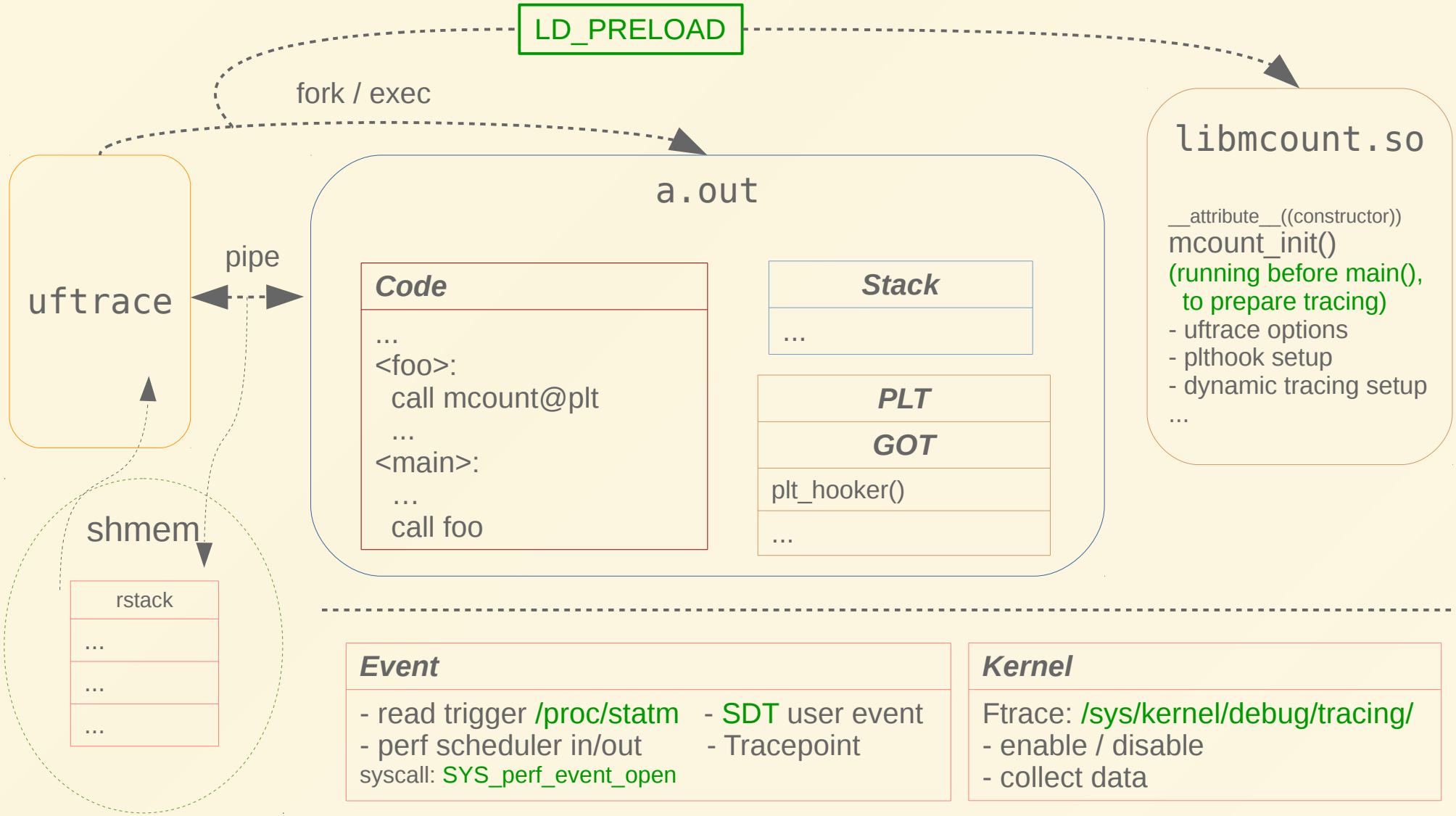
Thank you

treeze.taeung@gmail.com
taeung@kosslab.kr

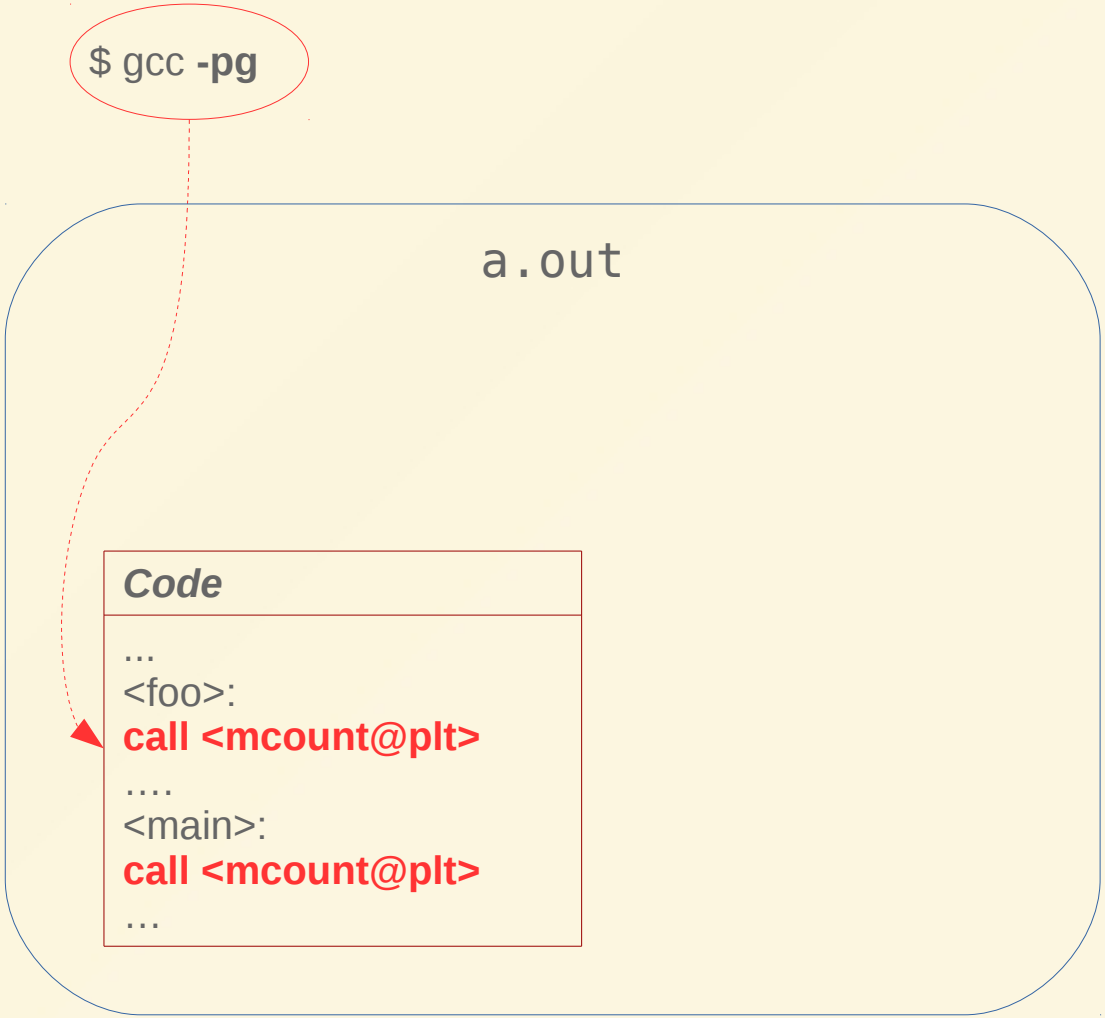
https://github.com/namhyung/uftrace

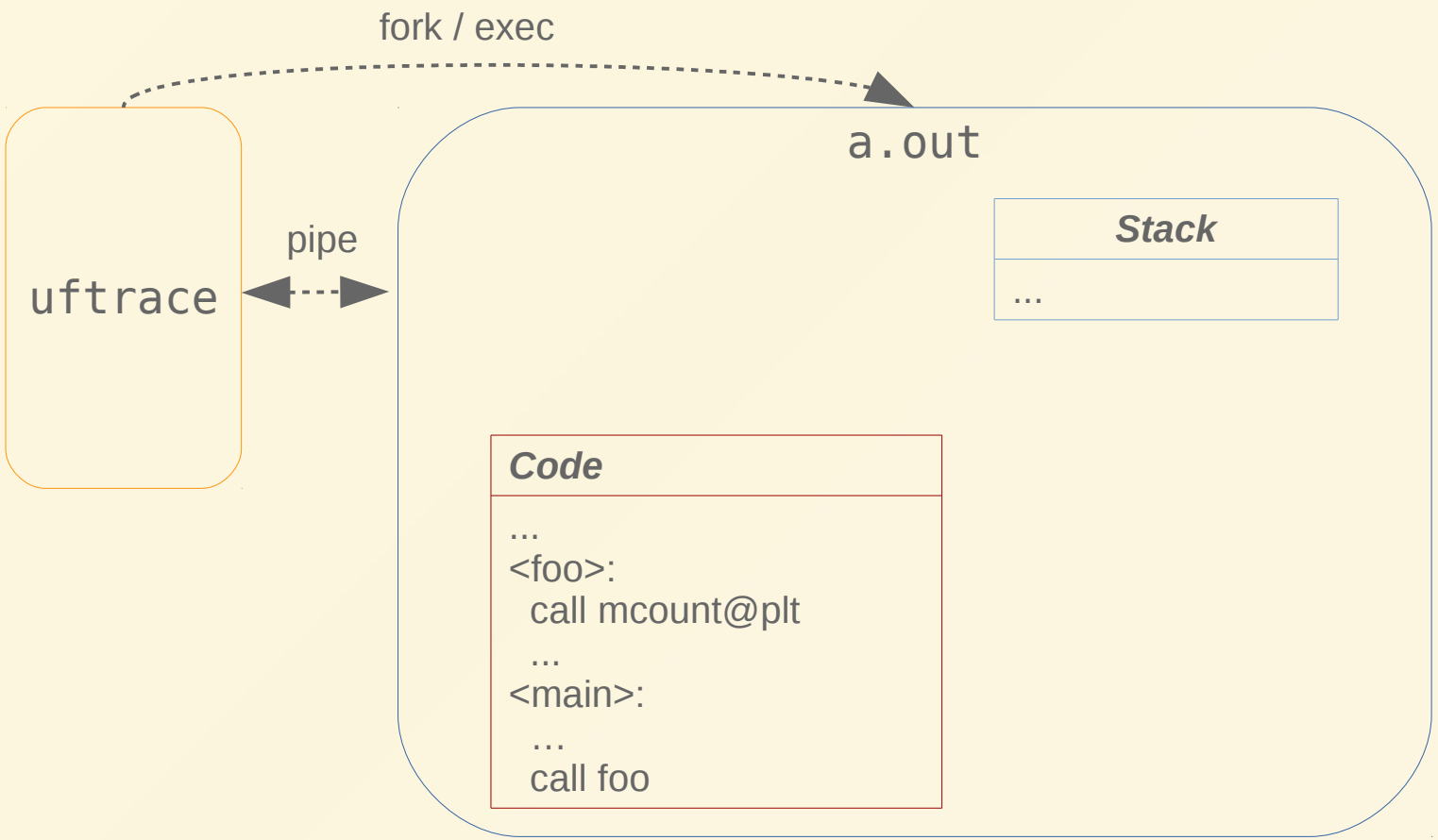
Appendix

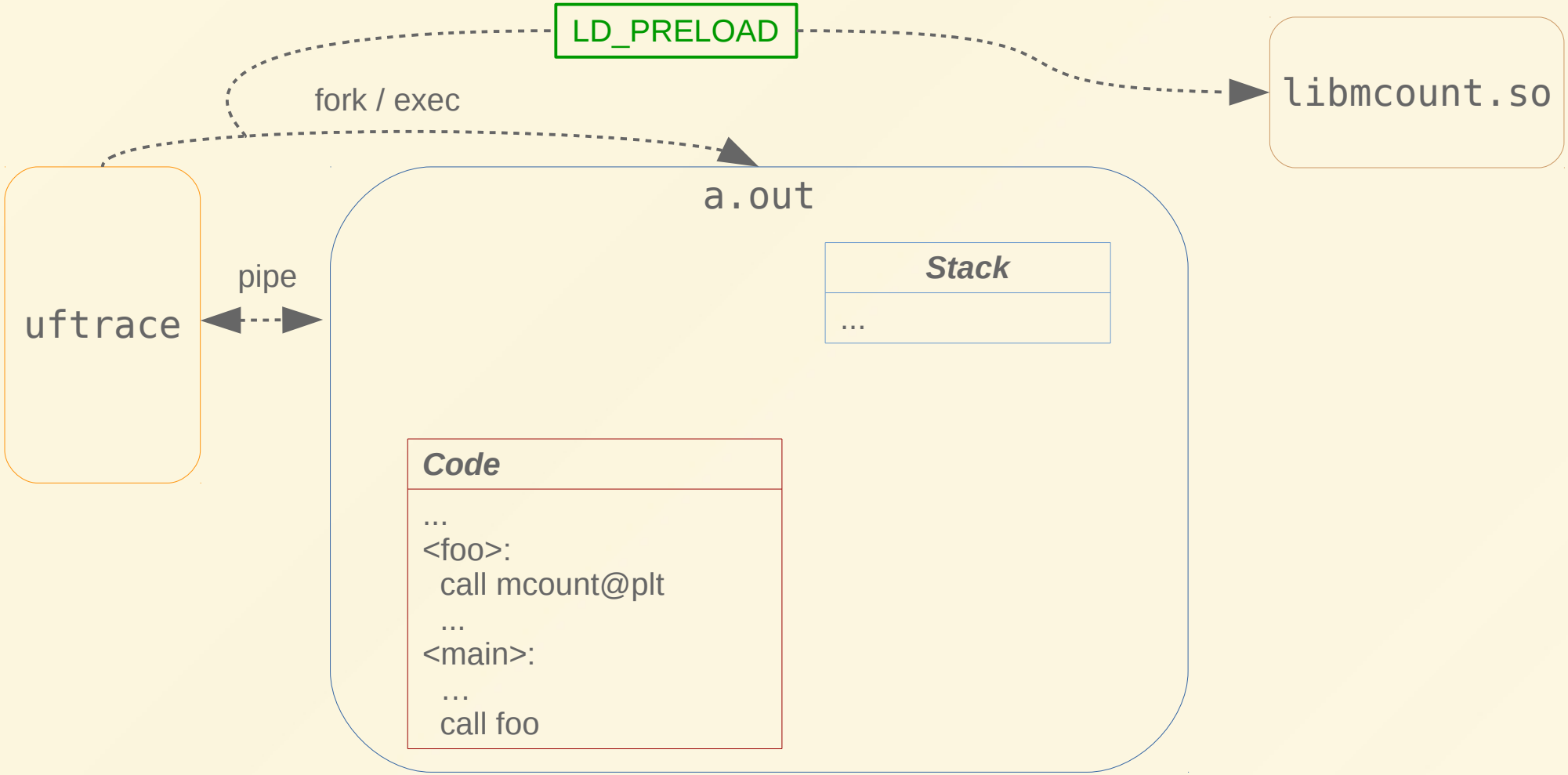
uftrace Internals

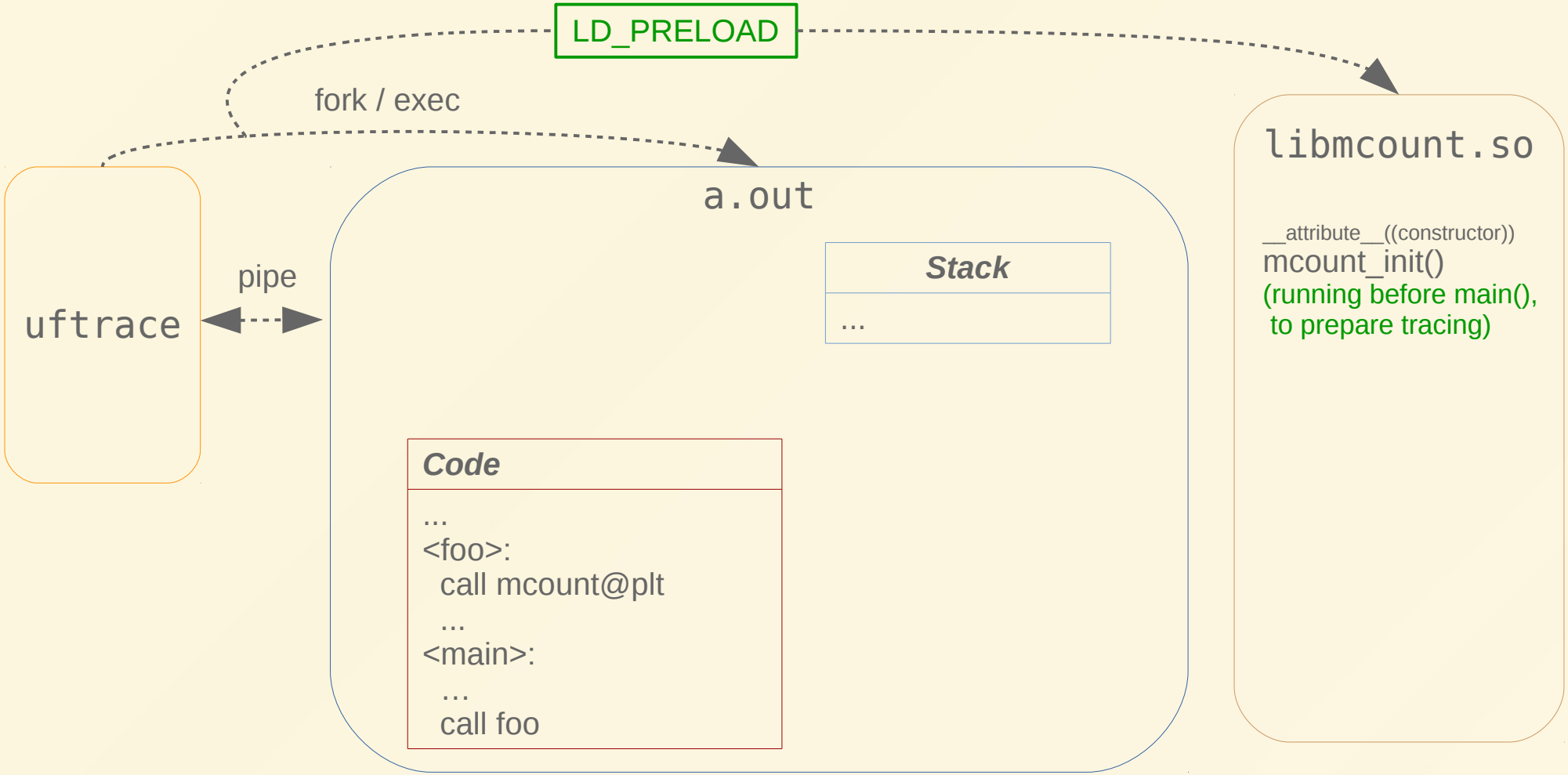

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
- uftrace options
- plthook setup
- dynamic tracing setup
...
uftrace
pipe
a.out
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo
Stack
...
PLT
GOT
plt_hooker()
...
shmem
rstack
...
...
...
Event
- read trigger /proc/statm
- perf scheduler in/out
syscall: SYS_perf_event_open
- SDT user event
- Tracepoint
Kernel
Ftrace: /sys/kernel/debug/tracing/
- enable / disable
- collect data

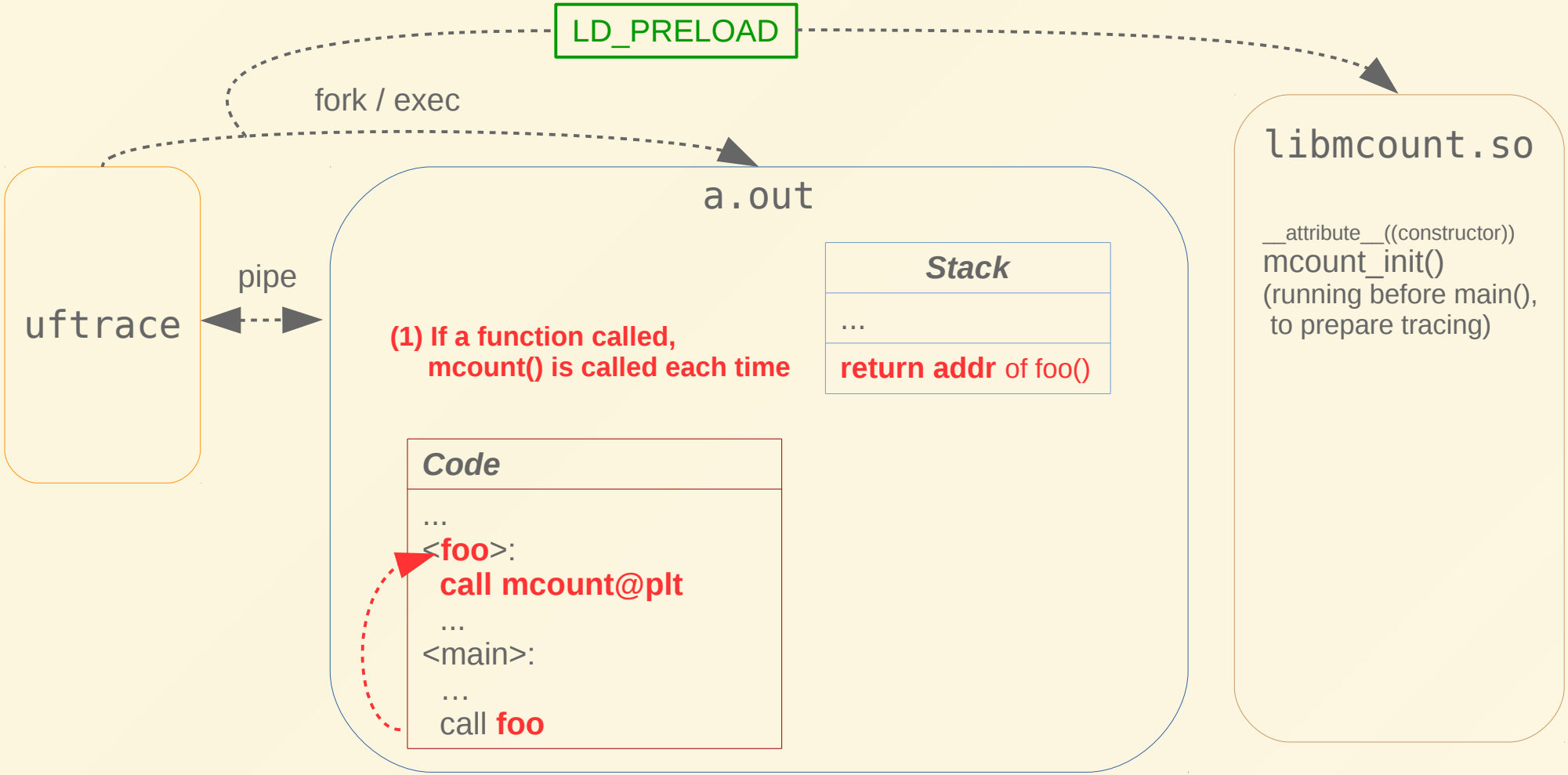
mcount hooking (user space function tracing)

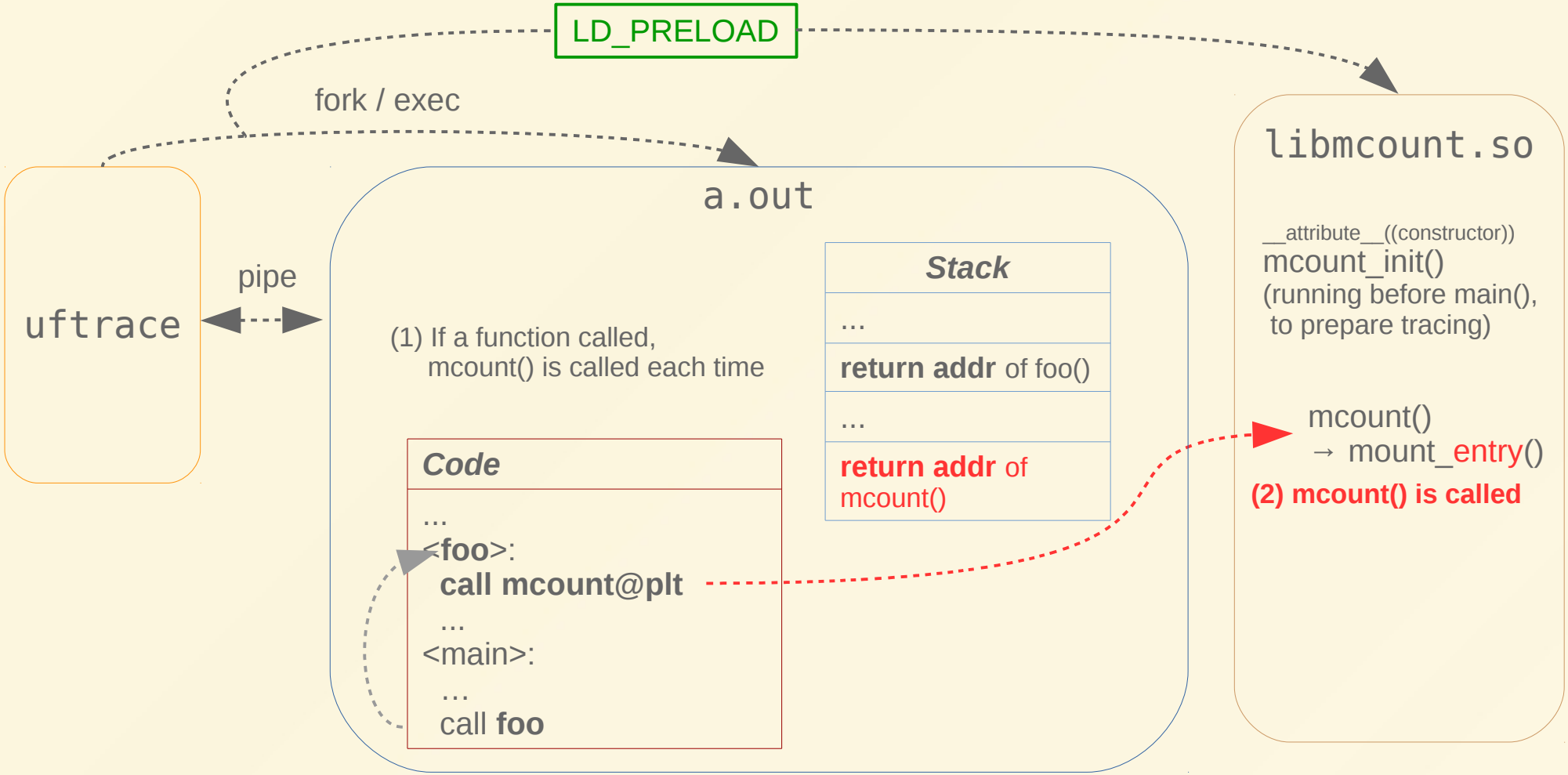

$ gcc -pg
a.out
Code
...
<foo>:
call <mcount@plt>
....
<main>:
call <mcount@plt>
...

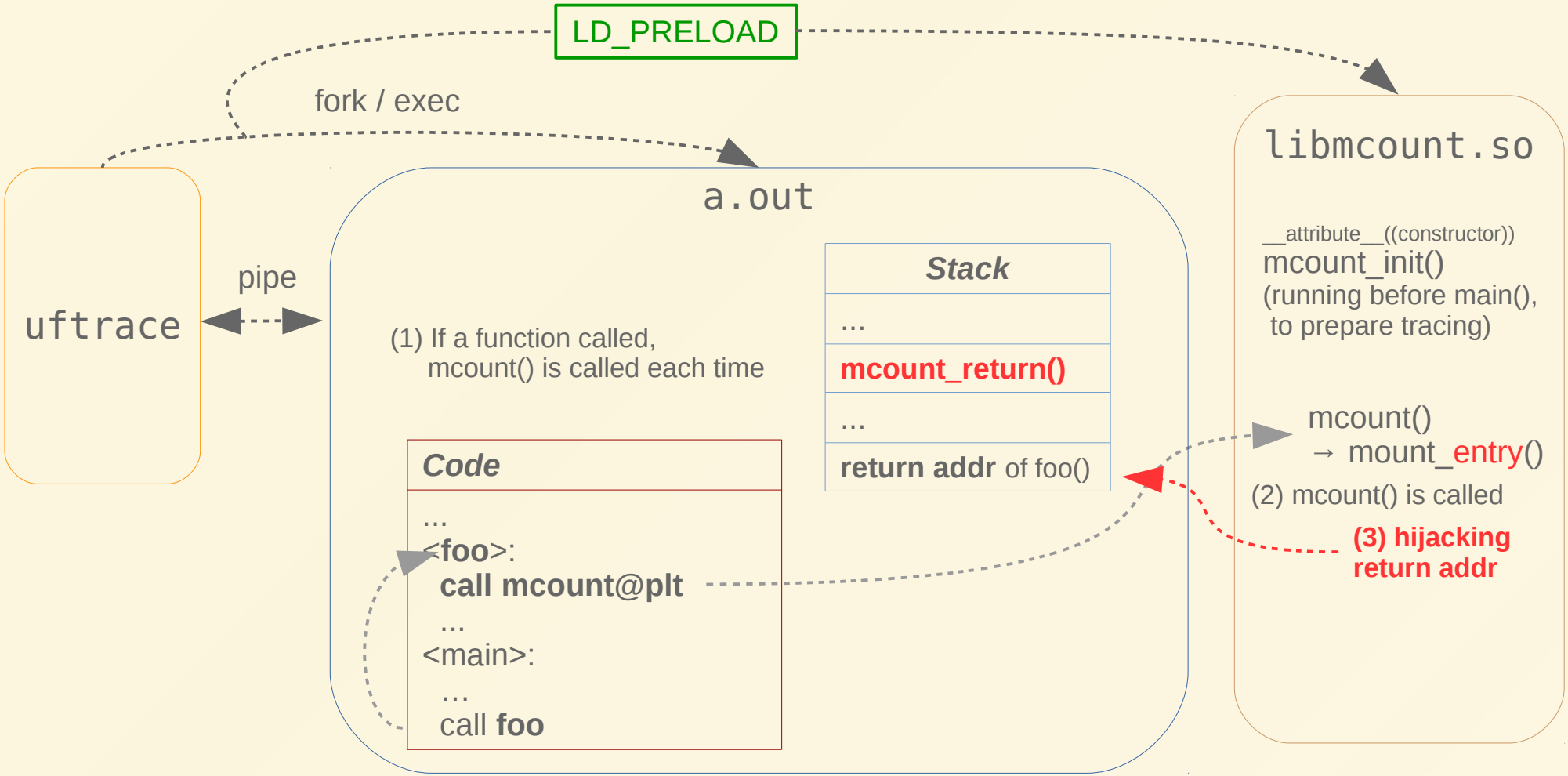

fork / exec
uftrace
pipe
a.out
Stack
...
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo

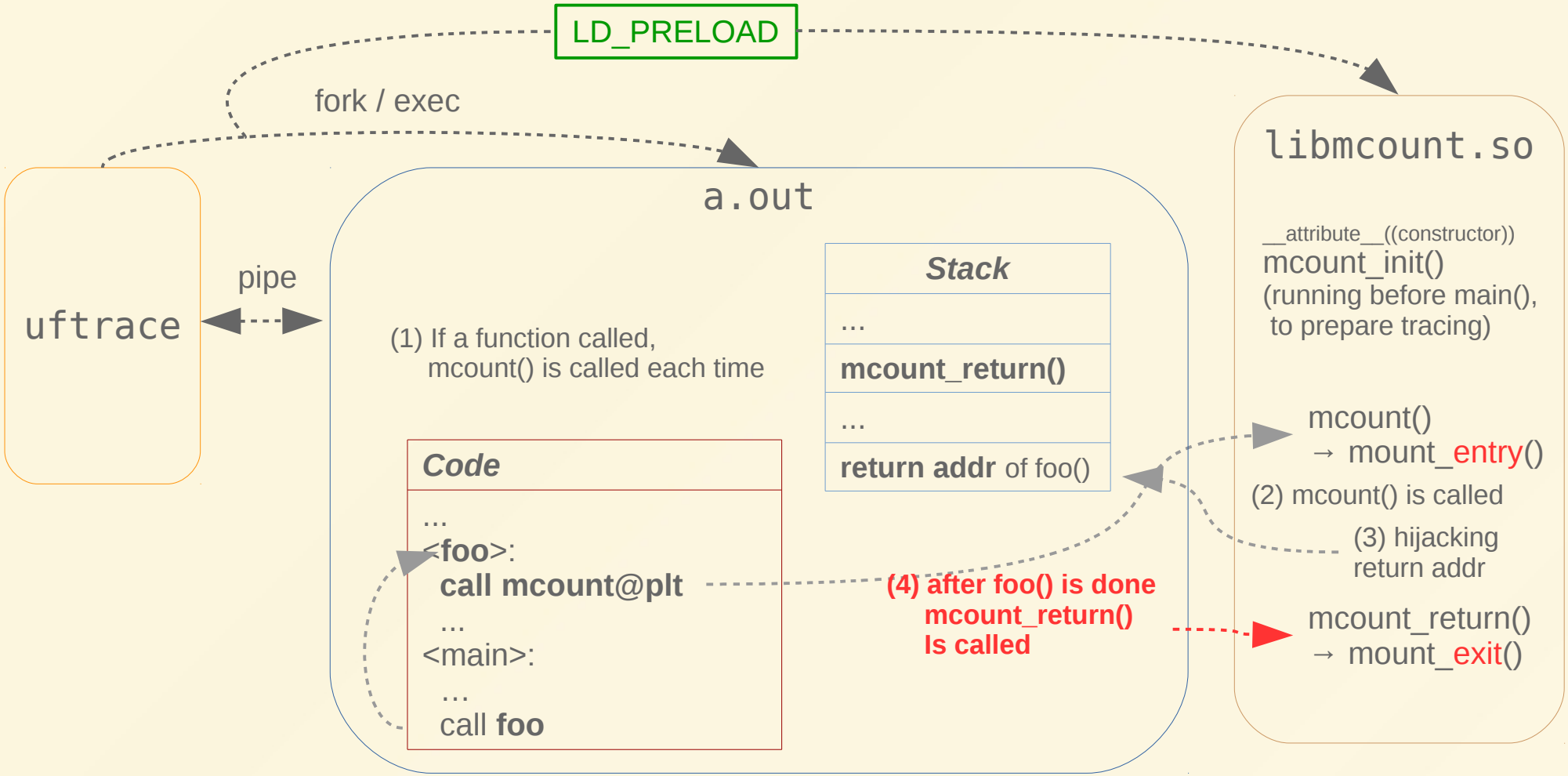

LD_PRELOAD
libmcount.so
fork / exec
a.out
uftrace
pipe
Stack
...
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo

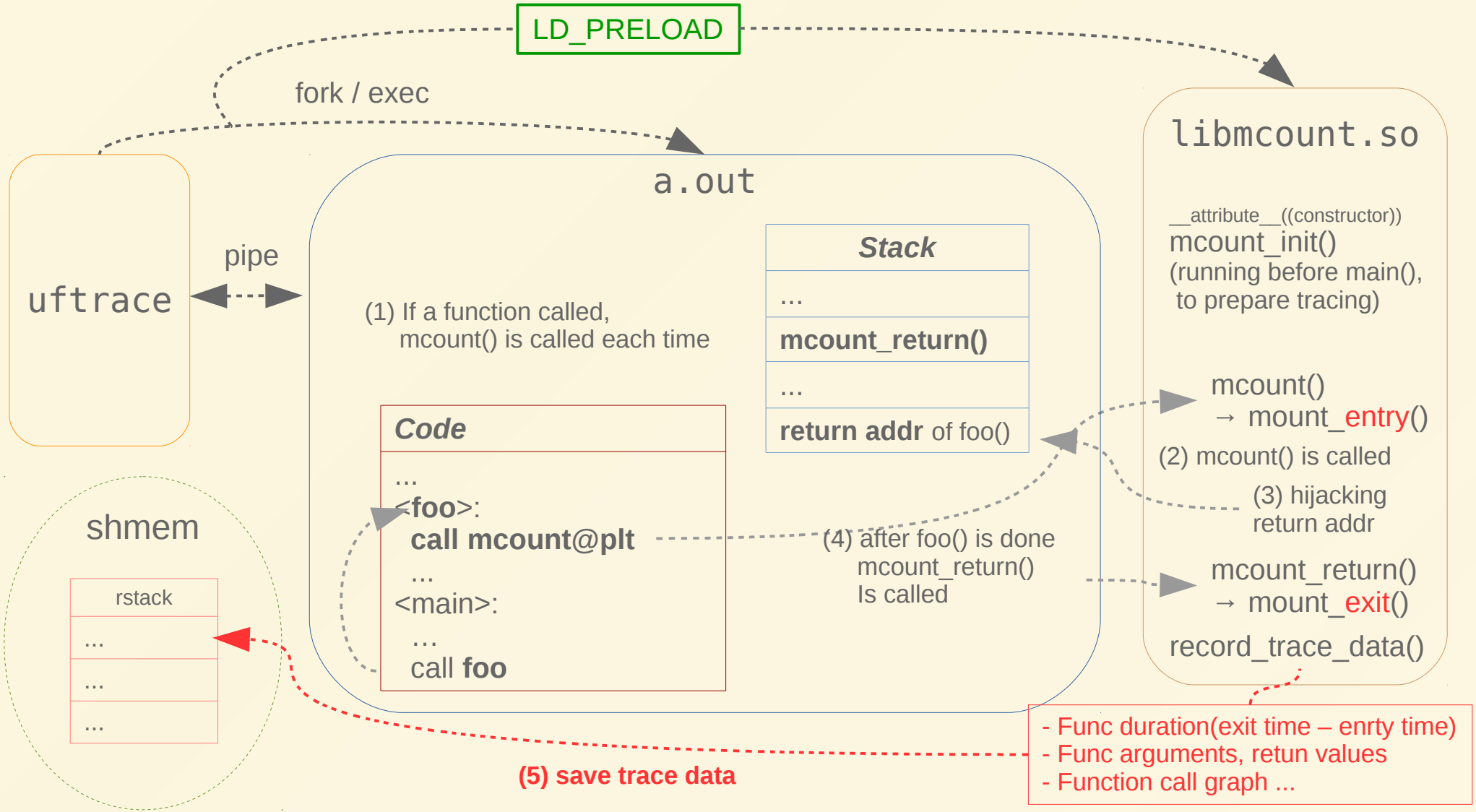

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
a.out
Stack
...
uftrace
pipe
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo

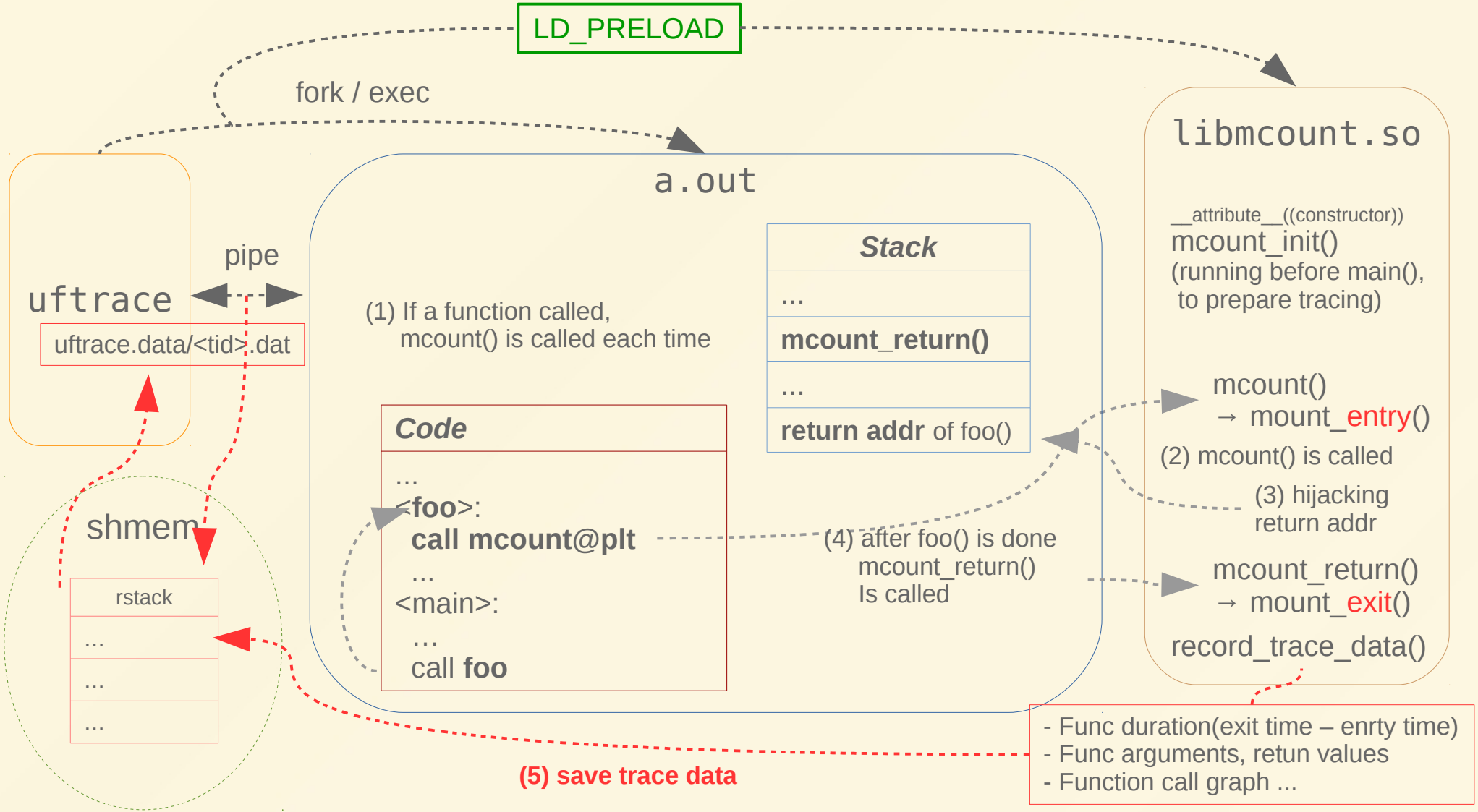

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
a.out
uftrace
pipe
Stack
...
return addr of foo()
(1) If a function called,
mcount() is called each time
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo


LD_PRELOAD
fork / exec
libmcount.so
a.out
uftrace
pipe
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
Stack
...
return addr of foo()
...
return addr of mcount()
(1) If a function called,
mcount() is called each time
mcount()
→ mount_entry()
(2) mcount() is called
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo

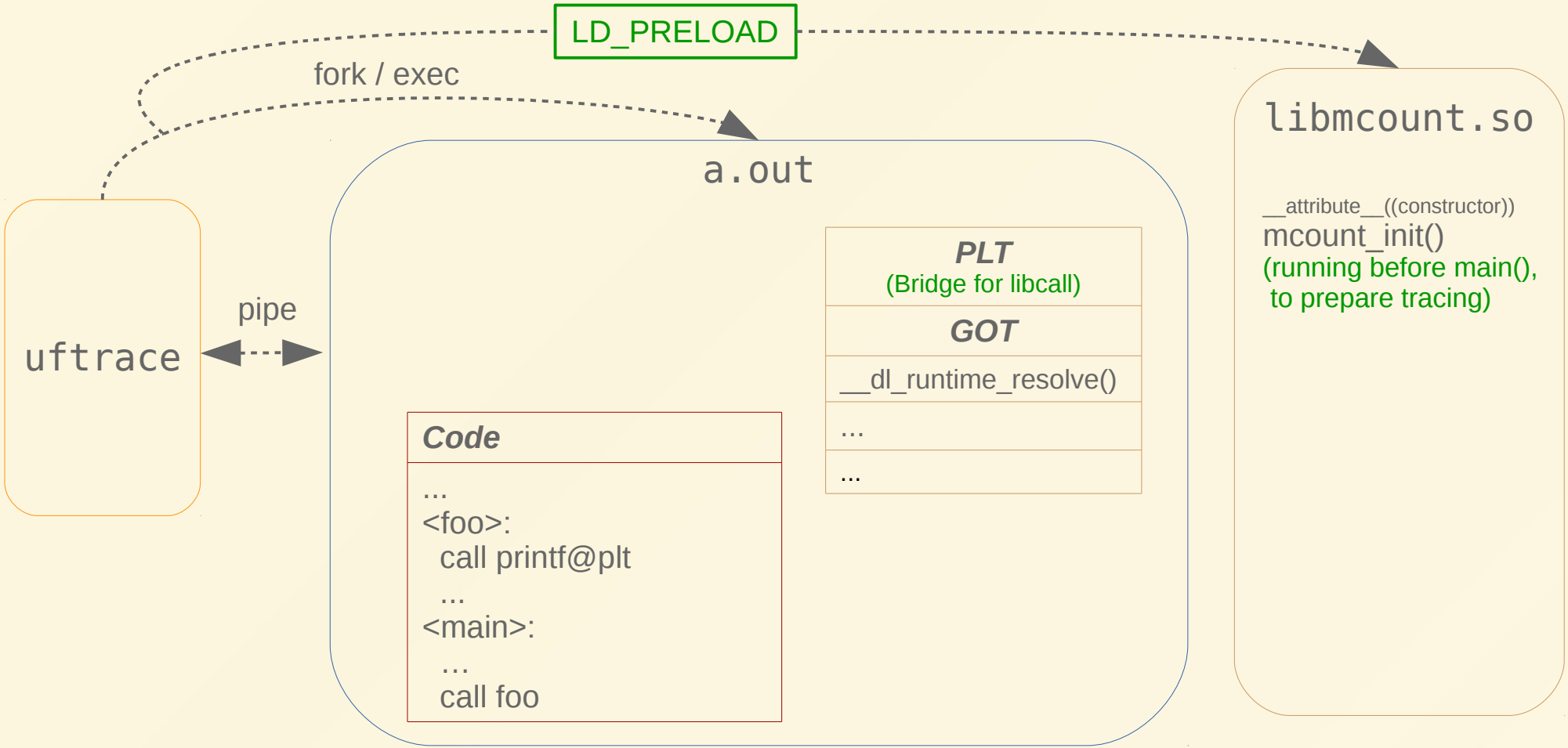

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
a.out
uftrace
pipe
(1) If a function called,
mcount() is called each time
Stack
...
mcount_return()
...
return addr of foo()
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo
mcount()
→ mount_entry()
(2) mcount() is called
(3) hijacking
return addr

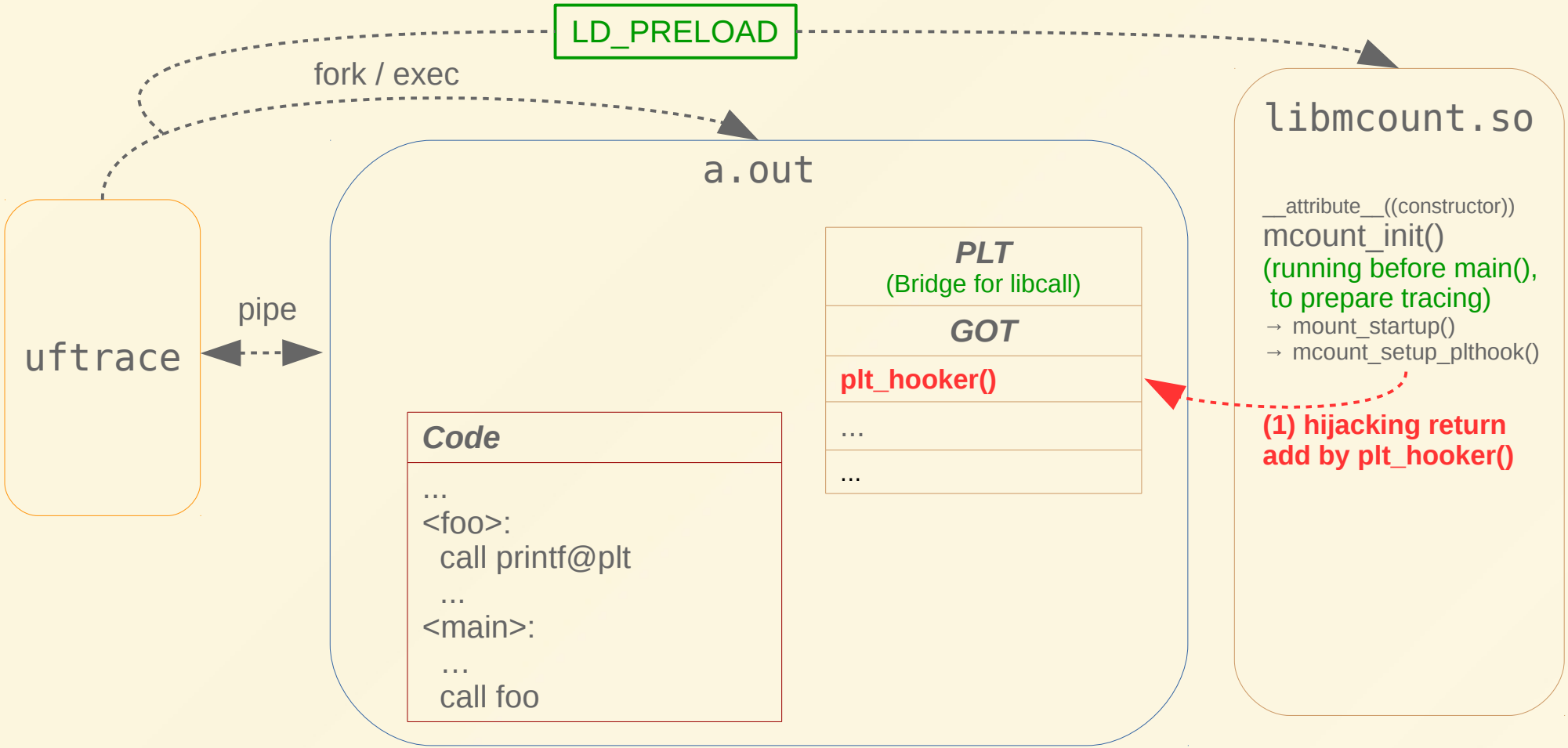

LD_PRELOAD
fork / exec
libmcount.so
a.out
uftrace
pipe
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
Stack
...
mcount_return()
...
return addr of foo()
(1) If a function called,
mcount() is called each time
mcount()
→ mount_entry()
(2) mcount() is called
(3) hijacking
return addr
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo
(4) after foo() is done
mcount_return()
Is called
mcount_return()
→ mount_exit()

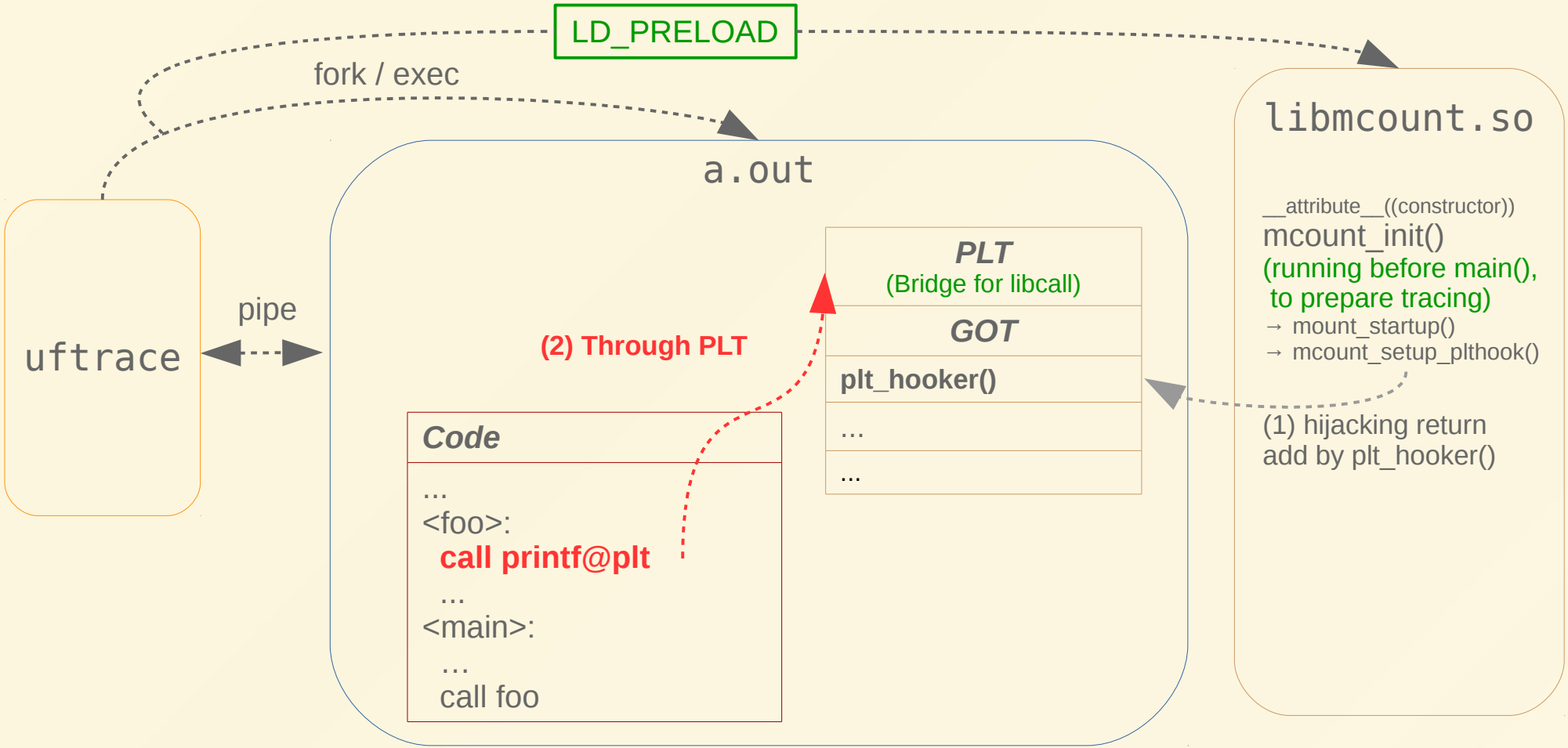

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
a.out
uftrace
pipe
Stack
...
mcount_return()
...
return addr of foo()
(1) If a function called,
mcount() is called each time
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo
mcount()
→ mount_entry()
(2) mcount() is called
(3) hijacking
return addr
(4) after foo() is done
mcount_return()
Is called
mcount_return()
→ mount_exit()
record_trace_data()
shmem
rstack
...
...
...
(5) save trace data
- Func duration(exit time – enrty time)
- Func arguments, retun values
- Function call graph ...

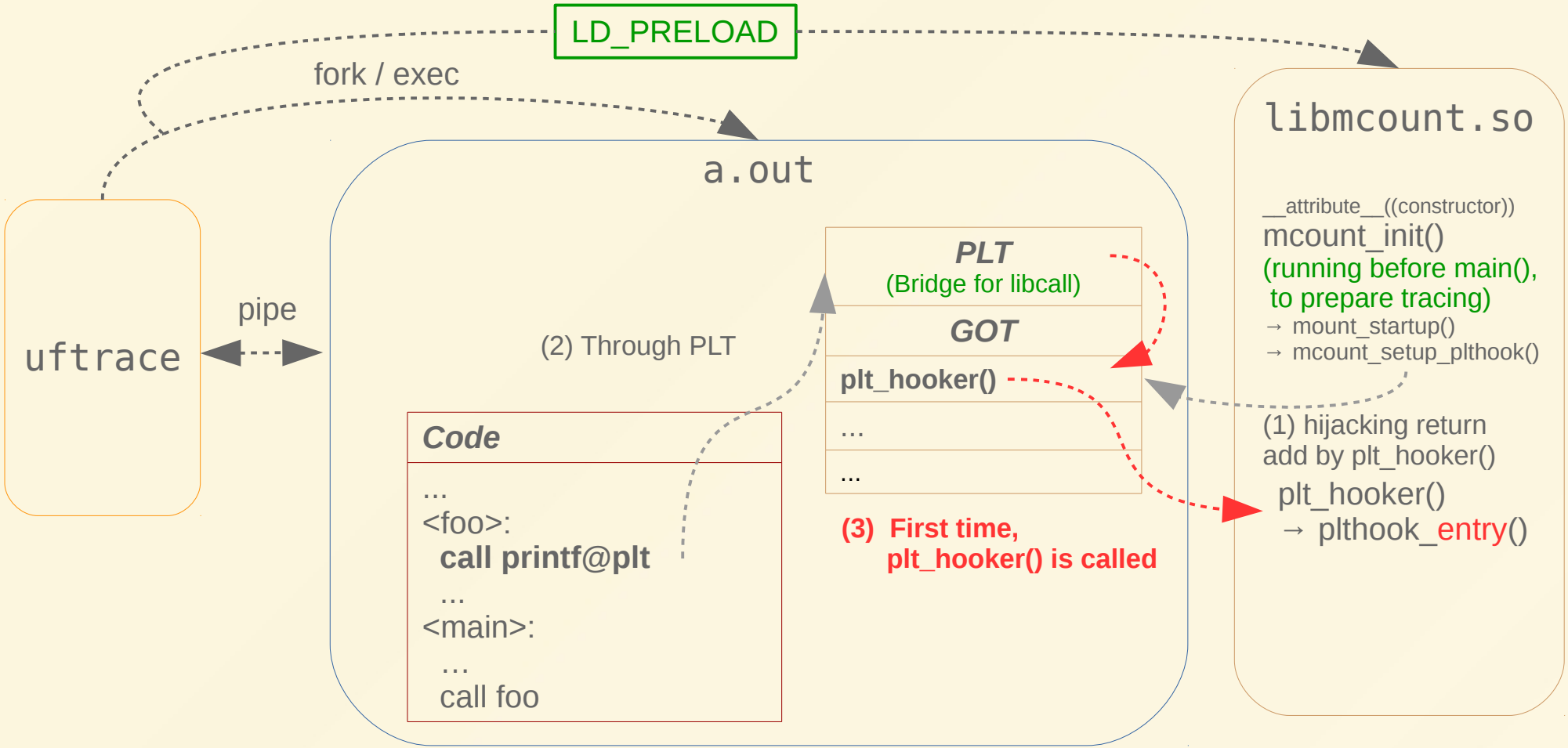

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
a.out
pipe
uftrace
uftrace.data/<tid>.dat
(1) If a function called,
mcount() is called each time
Stack
...
mcount_return()
...
return addr of foo()
Code
...
<foo>:
call mcount@plt
...
<main>:
...
call foo
mcount()
→ mount_entry()
(2) mcount() is called
(3) hijacking
return addr
(4) after foo() is done
mcount_return()
Is called
mcount_return()
→ mount_exit()
record_trace_data()
shmem
rstack
...
...
...
(5) save trace data
- Func duration(exit time – enrty time)
- Func arguments, retun values
- Function call graph ...

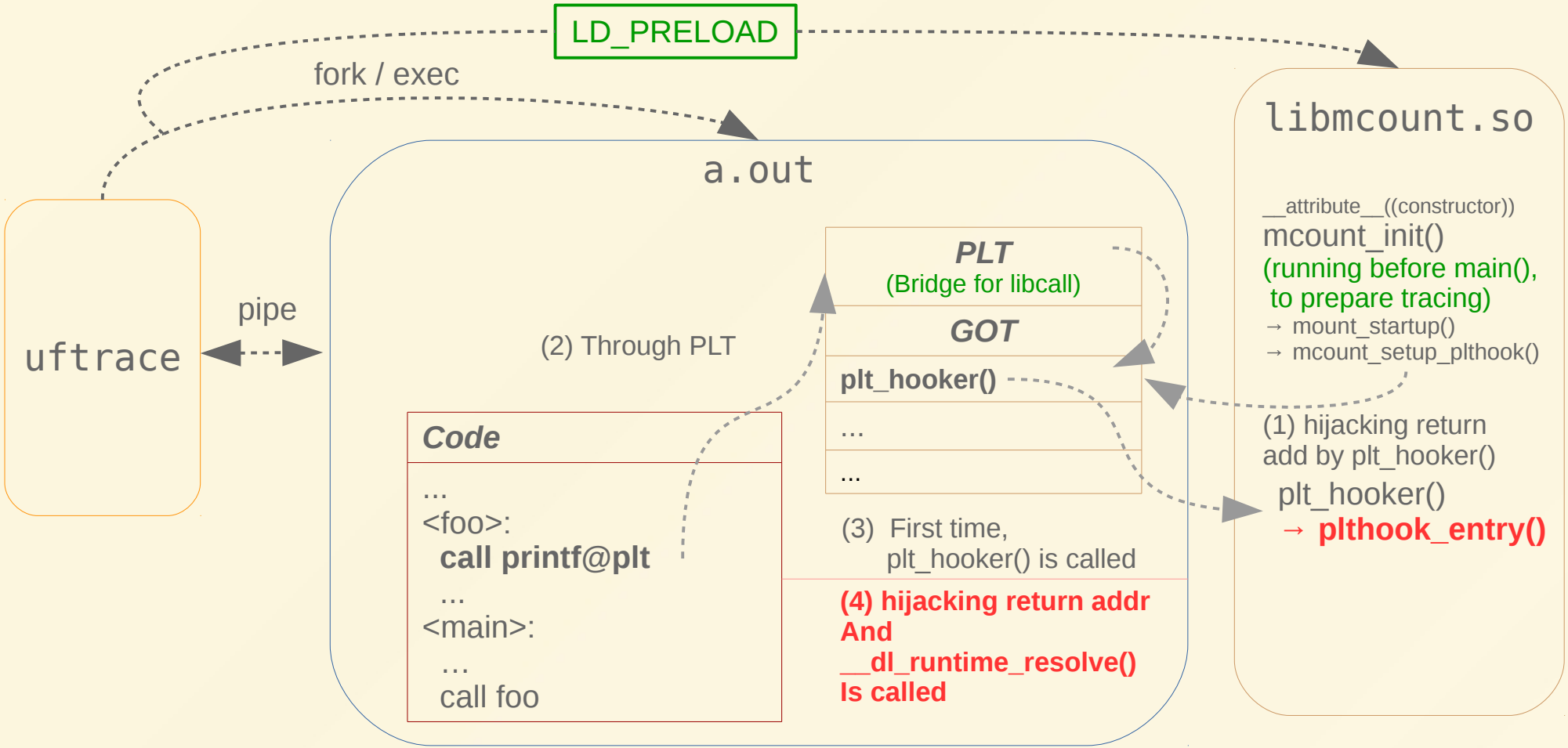
PLT hooking (library call tracing)

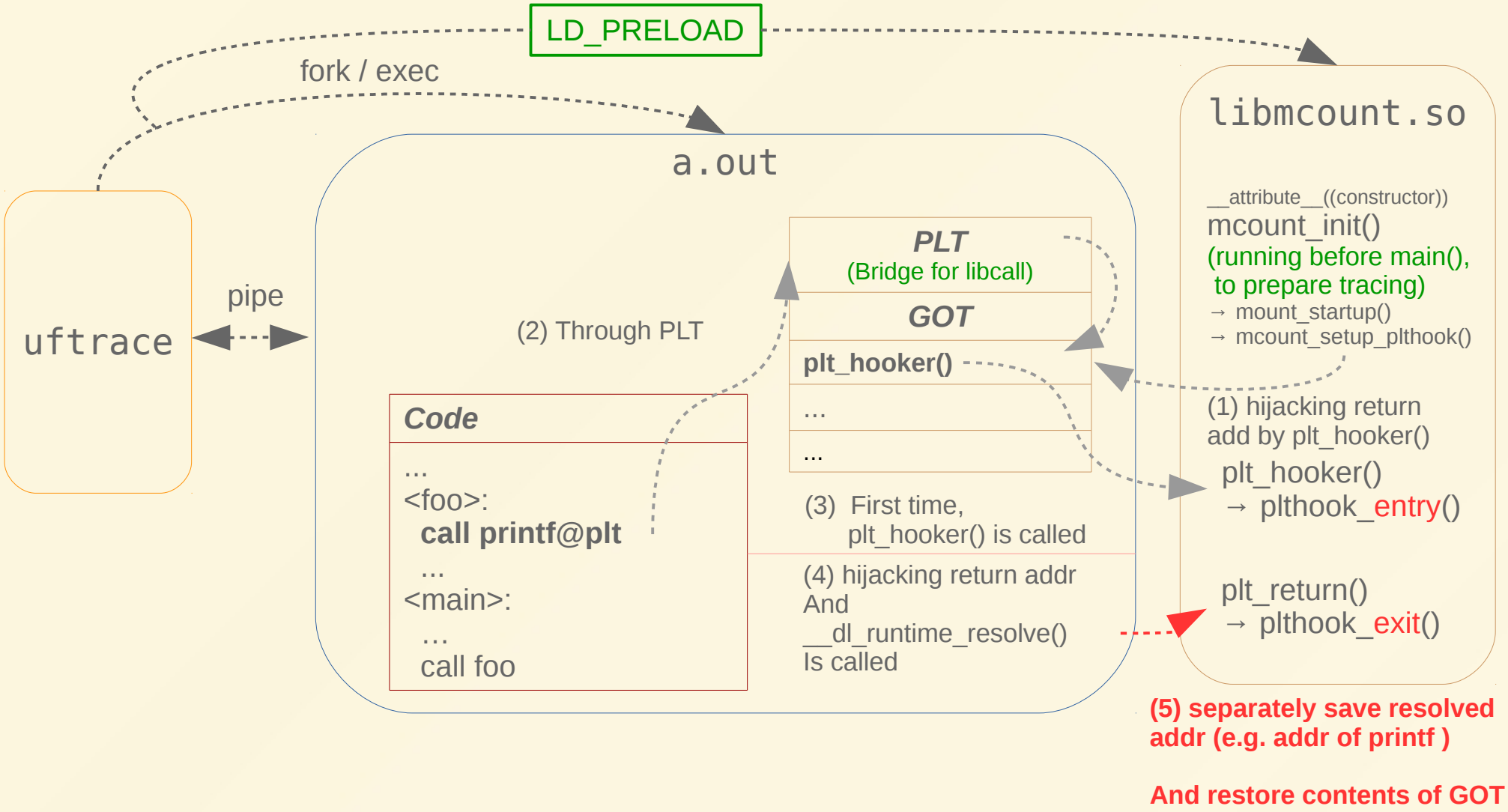

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
a.out
PLT
(Bridge for libcall)
GOT
__dl_runtime_resolve()
...
...
Code
...
<foo>:
call printf@plt
...
<main>:
...
call foo
pipe
uftrace

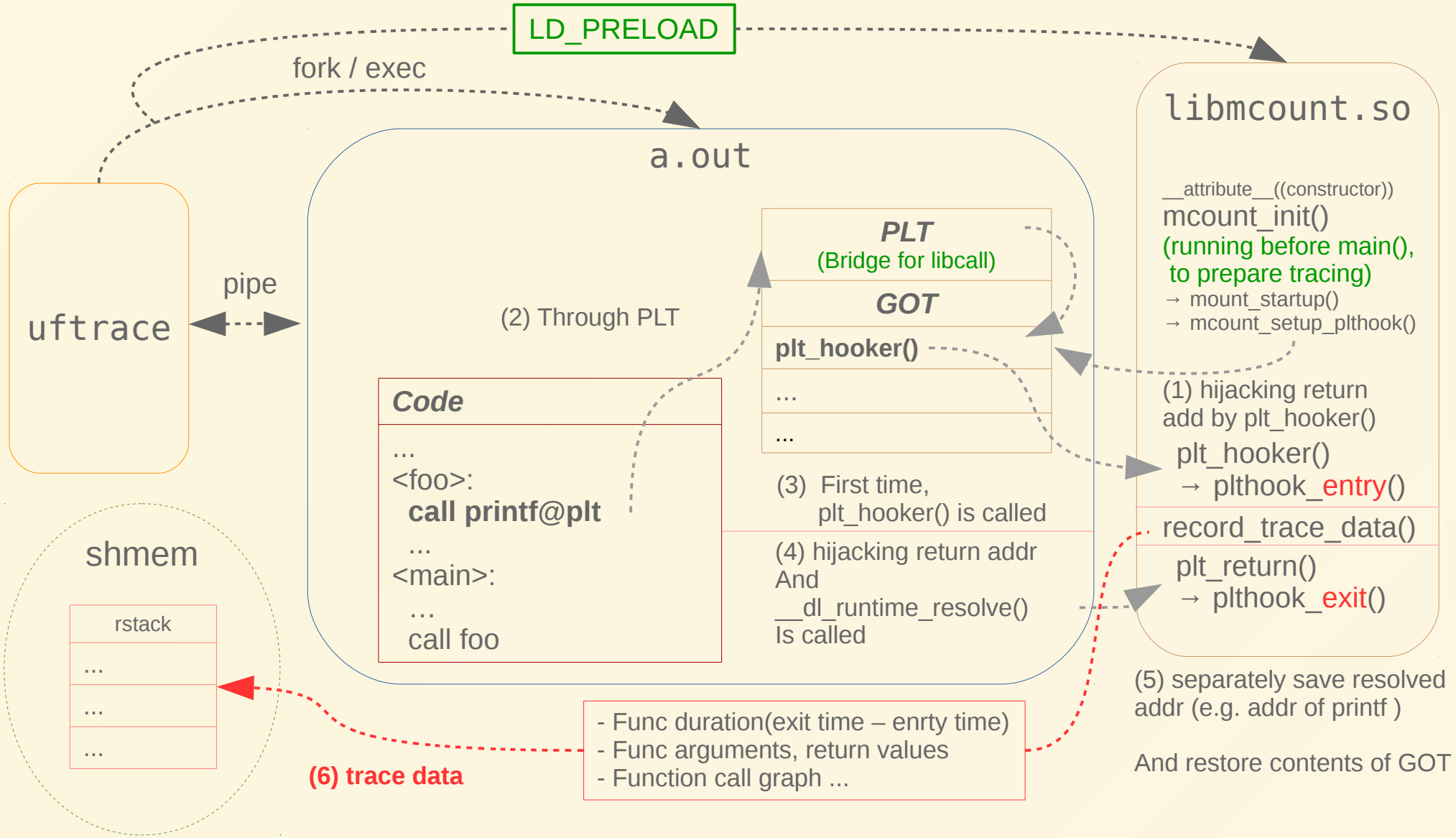

LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
→ mount_startup()
→ mcount_setup_plthook()
a.out
PLT
(Bridge for libcall)
GOT
plt_hooker()
...
...
Code
...
<foo>:
call printf@plt
...
<main>:
...
call foo
uftrace
pipe
(1) hijacking return
add by plt_hooker()


LD_PRELOAD
fork / exec
libmcount.so
a.out
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
→ mount_startup()
→ mcount_setup_plthook()
PLT
(Bridge for libcall)
GOT
plt_hooker()
...
...
(2) Through PLT
uftrace
pipe
Code
...
<foo>:
call printf@plt
...
<main>:
...
call foo
(1) hijacking return
add by plt_hooker()


LD_PRELOAD
fork / exec
libmcount.so
a.out
uftrace
pipe
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
→ mount_startup()
→ mcount_setup_plthook()
PLT
(Bridge for libcall)
GOT
plt_hooker()
...
...
(2) Through PLT
Code
...
<foo>:
call printf@plt
...
<main>:
...
call foo
(3) First time,
plt_hooker() is called
(1) hijacking return
add by plt_hooker()
plt_hooker()
→ plthook_entry()


LD_PRELOAD
fork / exec
libmcount.so
a.out
uftrace
pipe
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
→ mount_startup()
→ mcount_setup_plthook()
PLT
(Bridge for libcall)
GOT
plt_hooker()
...
...
(2) Through PLT
Code
...
<foo>:
call printf@plt
...
<main>:
...
call foo
(1) hijacking return
add by plt_hooker()
plt_hooker()
→ plthook_entry()
(3) First time,
plt_hooker() is called
(4) hijacking return addr
And
__dl_runtime_resolve()
Is called


LD_PRELOAD
fork / exec
libmcount.so
a.out
uftrace
pipe
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
→ mount_startup()
→ mcount_setup_plthook()
PLT
(Bridge for libcall)
GOT
plt_hooker()
...
...
(2) Through PLT
Code
...
<foo>:
call printf@plt
...
<main>:
...
call foo
(1) hijacking return
add by plt_hooker()
plt_hooker()
→ plthook_entry()
(3) First time,
plt_hooker() is called
(4) hijacking return addr
And
__dl_runtime_resolve()
Is called
plt_return()
→ plthook_exit()
(5) separately save resolved
addr (e.g. addr of printf)
And restore contents of GOT


LD_PRELOAD
fork / exec
libmcount.so
__attribute__((constructor))
mcount_init()
(running before main(),
to prepare tracing)
→ mount_startup()
→ mcount_setup_plthook()
a.out
uftrace
pipe
(2) Through PLT
PLT
(Bridge for libcall)
GOT
plt_hooker()
...
...
Code
...
<foo>:
call printf@plt
...
<main>:
...
call foo
(1) hijacking return
add by plt_hooker()
plt_hooker()
→ plthook_entry()
record_trace_data()
plt_return()
→ plthook_exit()
(3) First time,
plt_hooker() is called
(4) hijacking return addr
And
__dl_runtime_resolve()
Is called
shmem
rstack
...
...
...
(5) separately save resolved
addr (e.g. addr of printf)
And restore contents of GOT
(6) trace data
- Func duration(exit time – enrty time)
- Func arguments, return values
- Function call graph ...