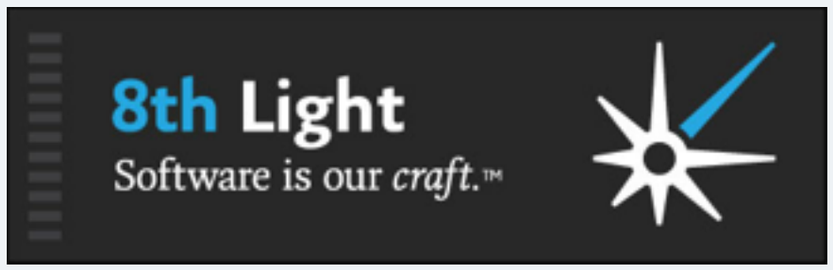
Finding out what's **really** going on, with DTrace!

Colin Jones
@trptcolin



What even is DTrace?

system-wide!

```
$ sudo dtrace -qn '
  syscall:::entry {
    @[probefunc, execname] = count();
  }
  dtrace:::END {
    trunc(@, 10); printa(@);
  }'
```

system-wide!

```
$ sudo dtrace -qn 'syscall:::entry { @[probefunc, execname] = count(); }
                   dtrace:::END { trunc(@, 10); printa(@); }'
^C

  read_nocancel                 dbfseventsd                   145
  workq_kernreturn              mds                           164
  kevent_qos                    Google Chrome He              170
  psynch_cvwait                 java                          197
  gettimeofday                  java                          199
  psynch_cvsignal               Box Sync                      264
  psynch_cvwait                 Box Sync                      265
  select                        Box Sync                      521
  kevent_qos                    hidd                          765
  stat64                        java                         1386
```

known events!

```
$ sudo dtrace -qn 'mysql*::: { @[probename] = count(); }
                   dtrace:::END { trunc(@, 10); printa(@); }'
^C

  query-exec-start                                                3
  query-parse-done                                                3
  query-parse-start                                               3
  query-start                                                     3
  select-done                                                     3
  select-start                                                    3
  net-read-done                                                  18
  net-read-start                                                 18
  net-write-done                                                 18
  net-write-start                                                18
```

arbitrary functions!
(aka **D**ynamic tracing)

```
$ sudo dtrace -n 'fbt:mach_kernel::entry { self->in = timestamp; }
                  fbt:mach_kernel::return /self->in/
                   { @ = quantize(timestamp - self->in) }'
dtrace: description 'fbt:mach_kernel::entry ' matched 24482 probes
^C
           value  ------------- Distribution ------------- count
             256 |                                         0
             512 |@@@@@@@@@@@@@@@@@@@@@@@@@@@              5591792
            1024 |@@@@@@@@@@                               2013056
            2048 |@@@@@@                                   1461593
            4096 |@                                        321681
            8192 |                                         31373
           16384 |                                         3764
           32768 |                                         2129
           65536 |                                         1331
          131072 |                                         749
          262144 |                                         485
          524288 |                                         394
         1048576 |                                         445
         2097152 |                                         438
         4194304 |                                         395
         8388608 |                                         104
        16777216 |                                         2
        33554432 |                                         0
```

Weird slowness...

it happens

Slooooooooow tests

(...sometimes)

Multiple tests, multiple machines

Affects some teammates worse than others

annoying
productivity-sapping
stressful

Hypotheses?

Use DTrace!

Rule out the usual suspect(s)

```
#!/usr/sbin/dtrace -s

#pragma D option quiet
#pragma D option switchrate=10hz

dtrace:::BEGIN
{
  printf("%-8s %s\n", "PID", "GC (ms)");
  self->start = 0;
}

hotspot*:::gc-begin
{
  self->start = timestamp;
}

hotspot*:::gc-end
/self->start/
{
  this->time = (timestamp - self->start) / 1000000;
  printf("%-8d %-8d\n", pid, this->time);
}
```

~~Garbage Collection~~

```
$ sudo gc_time.d
PID       GC (ms)
40320     9
40320     9
73113     1
73113     1
40320     36
73184     1
73184     1
73184     1
40320     9
40320     160
72735     7
```

CPU?

```
$ sudo dtrace -qn 'profile-997 { @[execname] = count(); }'
^C
  Alfred 2                                                1
  UserEventAgent                                          1
  mDNSResponder                                           1
  tmux                                                    1
  CrashPlanService                                        2
  launchd                                                 2
  symptomsd                                               2
  Box Sync                                                3
  Google Drive                                            3
  java                                                    3
  Google Chrome                                           9
  systemstatsd                                           11
  iTerm                                                  14
  Google Chrome He                                       24
  WindowServer                                           25
  hidd                                                   26
  Box Sync Monitor                                       47
  kernel_task                                          9527
```

CPU?

```
$ sudo dtrace -qn 'profile-997 /execname=="kernel_task"/
                     { @[stack()] = count(); }'
^C
[...]

  kernel`0xffffff80010f3d30+0x358
  kernel`0xffffff800158d890+0x793
  kernel`kevent+0x44
  kernel`unix_syscall64+0x251
  kernel`hndl_unix_scall64+0x16
  116

  kernel`processor_idle+0x107
  121

  kernel`machine_idle+0x2e0
  kernel`call_continuation+0x17
82967
```

~~CPU~~

```
$ sudo dtrace -qn 'profile-997 { @[execname] = count(); }'
^C
  Alfred 2                                                        1
  UserEventAgent                                                  1
  mDNSResponder                                                   1
  tmux                                                            1
  CrashPlanService                                                2
  launchd                                                         2
  symptomsd                                                       2
  Box Sync                                                        3
  Google Drive                                                    3
  java                                                            3
  Google Chrome                                                   9
  systemstatsd                                                   11
  iTerm                                                          14
  Google Chrome He                                               24
  WindowServer                                                   25
  hidd                                                           26
  Box Sync Monitor                                               47
  kernel_task                                                  9527
```

High-level resources

~~CPU~~

~~Memory~~

~~Disk~~

Network

Network connections

https://github.com/brendangregg/DTrace-book-scripts/blob/master/Chap6/soconnect_mac.d

```
$ sudo soconnect_mac.d
PID    PROCESS           FAM ADDRESS           PORT   LAT(us) RESULT
88161  java              2   127.0.0.1         5432       144 Success
88161  java              2   127.0.0.1         5432       171 Success
88161  java              2   127.0.0.1         5432       150 Success
114    AirPlayXPCHelper  2   192.168.1.27      7000      1762 In progress
88161  java              2   127.0.0.1         5432       141 Success
88161  java              2   127.0.0.1         5432       179 Success
88161  java              2   127.0.0.1         5432       137 Success
88161  java              2   72.52.4.119       80       29977 Success
88161  java              2   72.52.4.119       80       42121 Success
88161  java              2   72.52.4.119       80       29471 Success
88161  java              2   72.52.4.119       80       29360 Success
88161  java              2   72.52.4.119       80       34731 Success
88161  java              2   72.52.4.119       80       28824 Success
```

DNS

```
dtrace:::BEGIN
{
  printf("%-8s %-8s %s\n", "TICK", "ms", "HOST");
  timezero = timestamp;
}

pid$target::getaddrinfo:entry
{
  self->host = copyinstr(arg0);
  self->start = timestamp;
}

pid$target::getaddrinfo:return
/self->start/
{
  this->now = (timestamp - timezero) / 1000000;
  this->time = (timestamp - self->start) / 1000000;
  printf("%-8d %-8d %s\n", this->now, this->time, self->host);
  self->start = 0; self->host = 0;
}
```

```
$ sudo dns_latency.d -p 41161
Password:
TICK     ms       HOST
74450    274      redclay.local
74734    0        redclay.local
105006   30075    someplace.com
145171   30075    someplace.com
145191   1        redclay.local
145192   0        redclay.local
177055   0        example.com
252314   2        redclay.local
252315   0        redclay.local
284392   0        example.com
```

Now we know what to fix!

What did we learn?

DTrace gets you answers

You can do it!

Where can we learn more?

Read

Brendan Gregg's blog:
http://www.brendangregg.com/dtrace.html

The DTrace guide
http://dtrace.org/guide

Examples

Scripts that ship with OS X

`find /usr/bin -name "*.d"`

more DTrace scripts

https://github.com/brendangregg/DTrace-book-scripts

Extrapolate

Try it out!

Thanks!

Colin Jones
@trptcolin