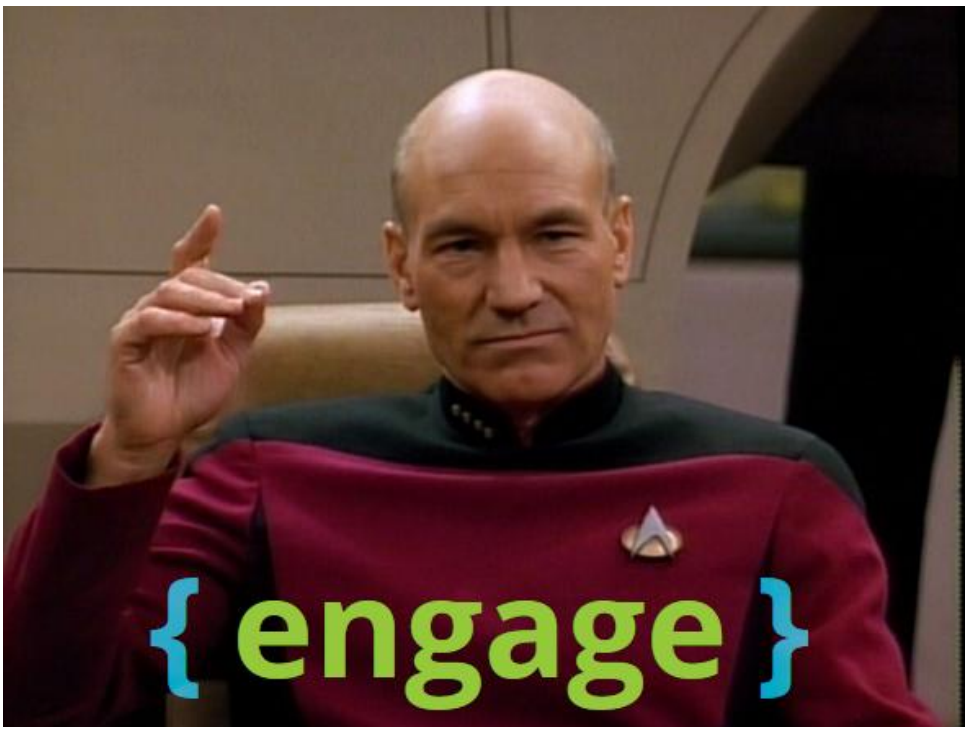
Remove and Prevent: Dealing with Bugs in Software and Systems

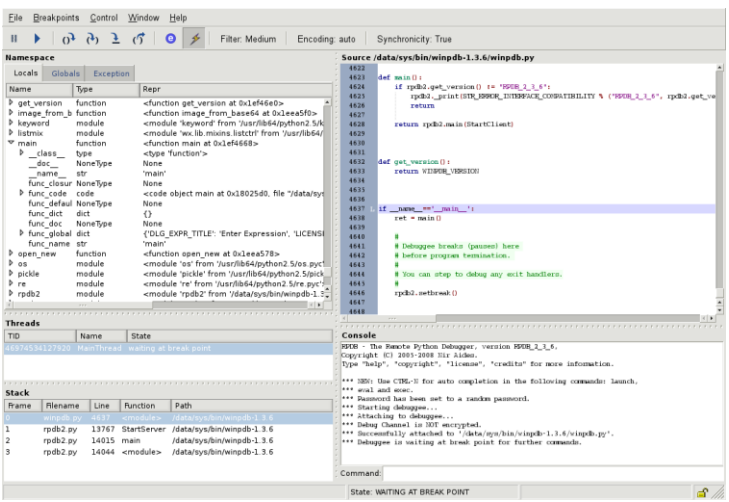
Diomidis Spinellis
Department of Management Science and Technology
Athens University of Economics and Business

www.spinellis.gr
dds@aueb.gr
@CoolSWEng



printk(KERN_WARNING "Dodgy doffset!\n");

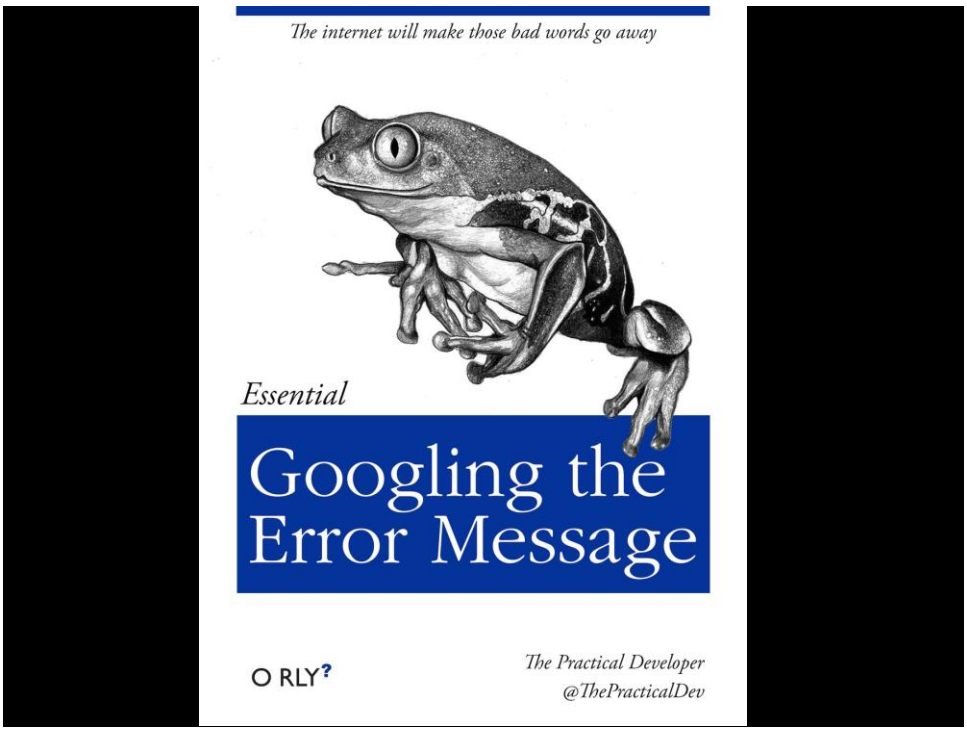
— Linux: drivers/nubus/nubus.c



6

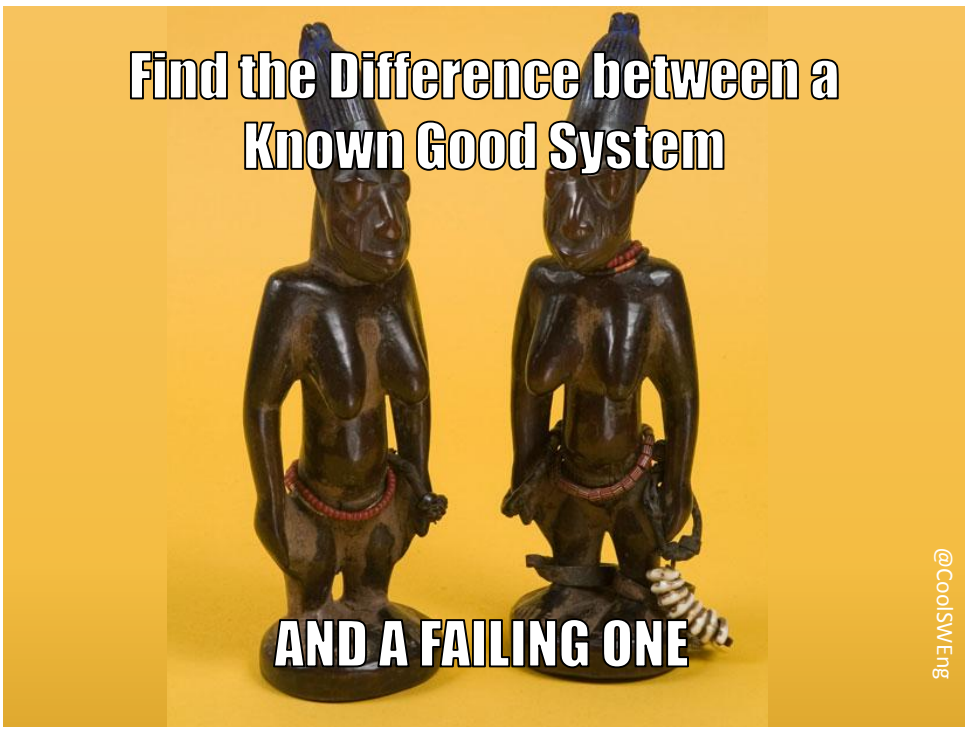

Strategies
GOT 'EM!


Handle All Problems through an Issue-Tracking System
OR DROWN BY THEM
Filters
is:issue is:open
Labels
Milestones
New issue
276 Open
3,703 Closed
Author
Labels
Milestones
Assignee
Sort
on start webview backe
#5175 opened on 15 Apr by jri
1
autoUpdater.quitAndInstall does not restart when app.makeSingleInstance is used
beginner bug windows
#5163 opened on 15 Apr by havenchyk
5
HTML5 drag-drop is now working un KUbuntu
blocked bug linux linux-distribution-specific
#5162 opened on 15 Apr by antelle
6
window.open allows a malicious script to read arbitrary local files
bug security
#5151 opened on 14 Apr by harupu
20
Error message includes local PC user name and can be accessed by injected script on remote server
bug security
#5148 opened on 14 Apr by harupu
0
window.close after print dialog closes all windows
bug crash linux
#5130 opened on 13 Apr by RobsonMi
1
Is it possible to get a WebFrame instance for a frame/iframe inside the current page?
enhancement
#5115 opened on 11 Apr by Mr0grog
1
2
2
#5110 opened on 11 Apr by elisee

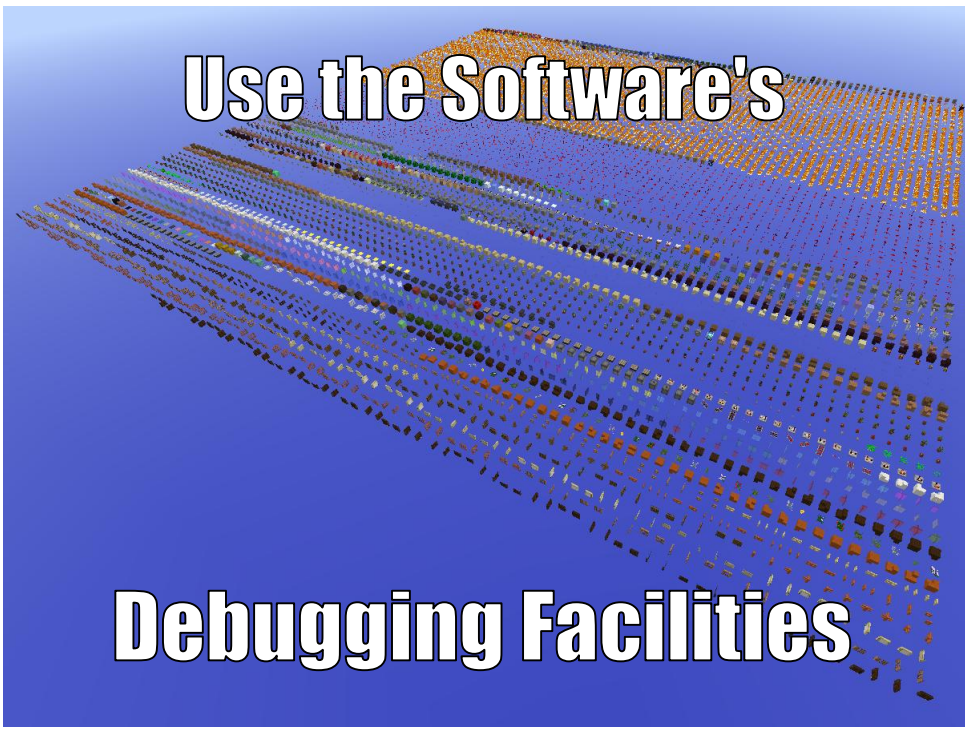

The internet will make those bad words go away
Essential
Googling the Error Message
O RLY?
The Practical Developer
@ThePracticalDev


Confirm That Preconditions and Postconditions
are Satisfied

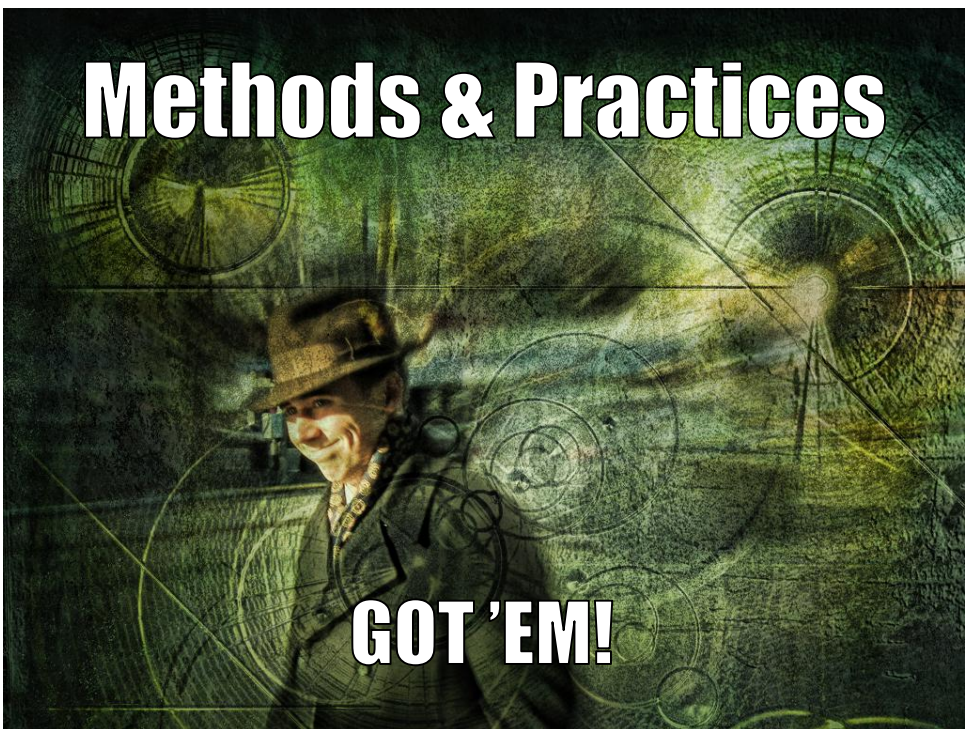

Drill Up
from the Problem to the Bug
or Down from the Program's Start
to the Bug
@CoolSWEng


Find the Difference between a
Known Good System
AND A FAILING ONE
@CoolSWEng

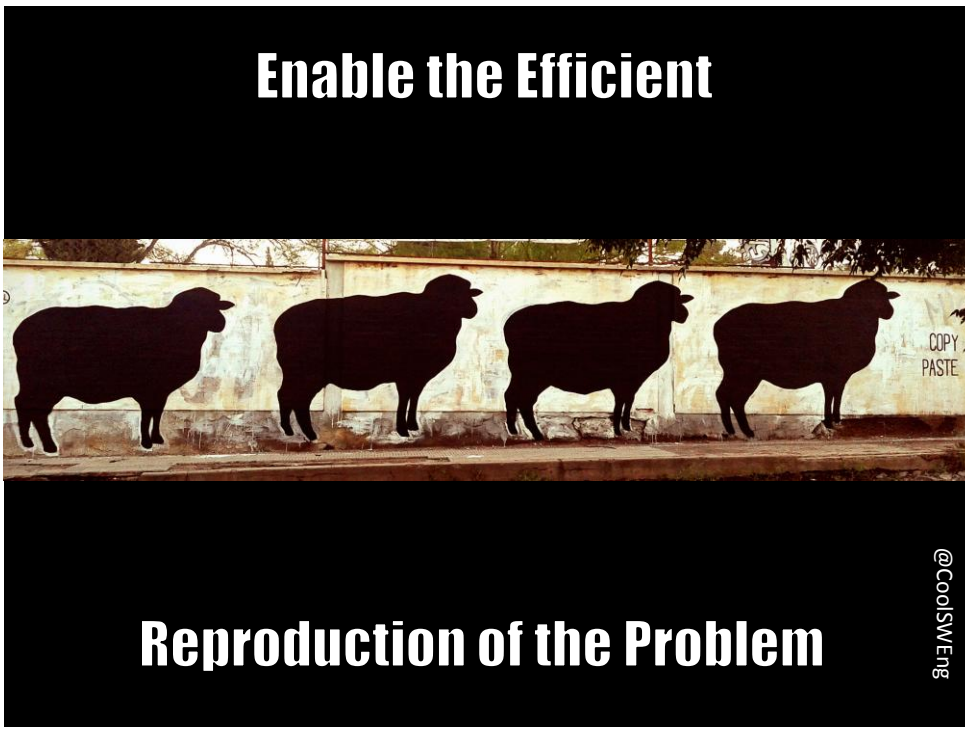
```
comm -23 <(
  awk '/open\(/ {print $2}' t1 |
  sort) \
        <(
  awk '/open\(/ {print $2}' t2 |
  sort)
```



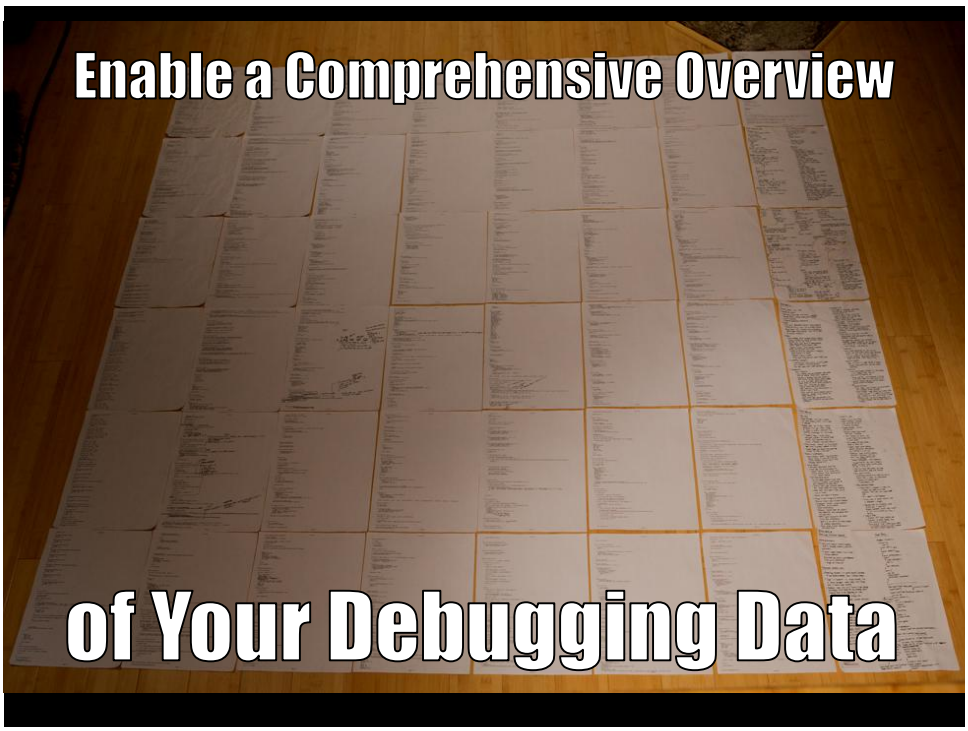

Minecraft 1.10 (1.10/vanilla)
77 fps (66 chunk updates) T: inf vbo
C: 576/67600 (s) D: 32, L: 0, pC: 000, pU: 2, aB: 59
E: 17/106, B: 0
P: 18, T: All: 106
MultiplayerChunkCache: 1300, 1300
XYZ: -324.687 / 70.00000 / 75.460
Block: -325 70 75
Chunk: 11 6 11 in -21 4 4
Facing: north (Towards negative Z) (136.2 / -3.2)
Biome: Plains
Light: 15 (15 sky, 0 block)
Local Difficulty: 1.50 // 0.00 (Day 0)
Debug: Pie [shift]: hidden FPS [alt]: hidden
For help: press F3 + Q
Java: 1.8.0_25 64bit
Mem: 6% 791/12743MB
Allocated: 8% 1144MB
CPU: 6x AMD FX(tm)-6350 Six-Core Processor
Display: 1920x1080 (ATI Technologies Inc.)
AMD Radeon (TM) R7 370 Series Graphics
4.5.13416 Compatibility Profile Context 15.300.1025.1001

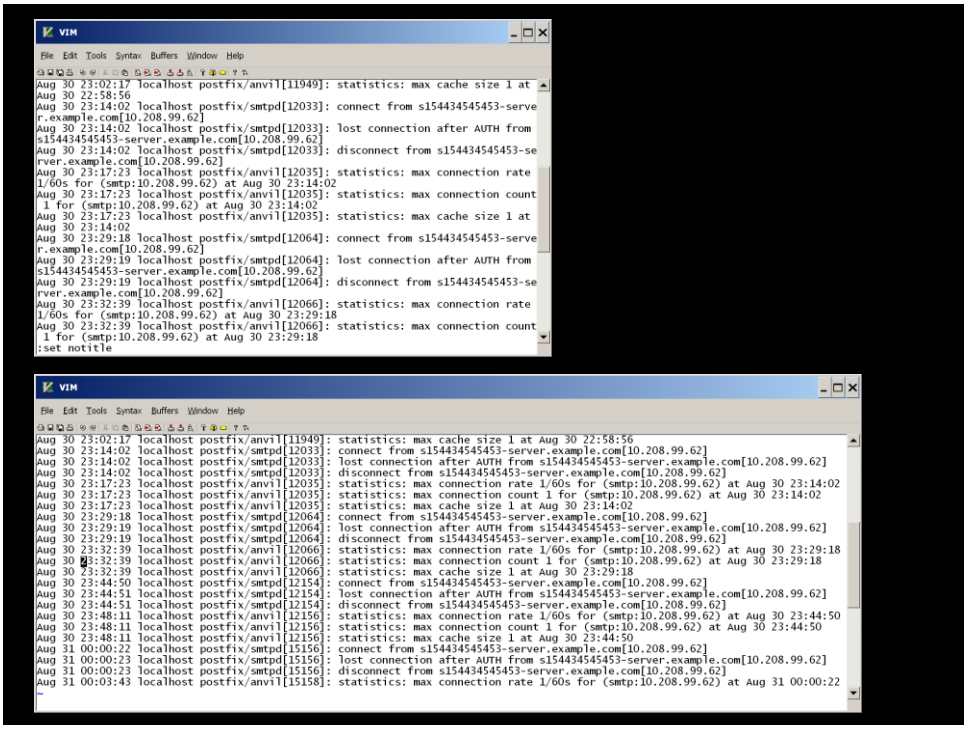

Methods & Practices
GOT 'EM!

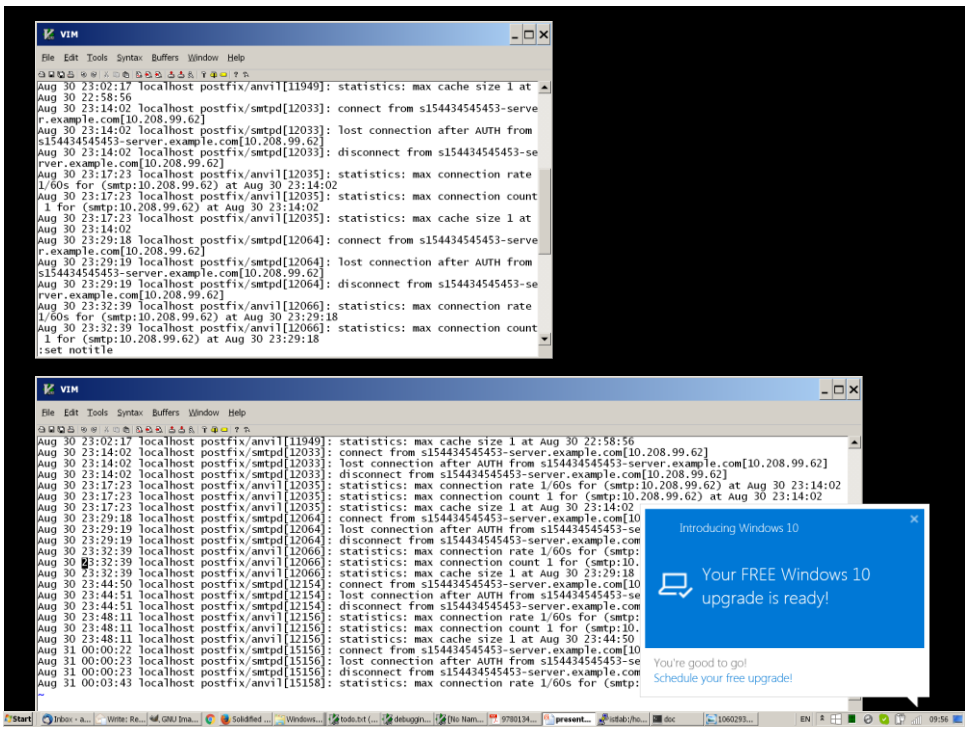

Set Yourself Up
for Debugging Success


Enable the Efficient
COPY
PASTE
Reproduction of the Problem
@CoolSWEng

```
mvn -Dtest=TestFetch test
```




VIM
File Edit Tools Syntax Buffers Window Help
Aug 30 23:02:17 localhost postfix/anvil[11949]: statistics: max cache size 1 at Aug 30 22:58:56
Aug 30 23:14:02 localhost postfix/smtpd[12033]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max cache size 1 at Aug 30 23:14:02
Aug 30 23:29:18 localhost postfix/smtpd[12064]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:29:18
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:29:18
:set notitle
VIM
File Edit Tools Syntax Buffers Window Help
Aug 30 23:02:17 localhost postfix/anvil[11949]: statistics: max cache size 1 at Aug 30 22:58:56
Aug 30 23:14:02 localhost postfix/smtpd[12033]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max cache size 1 at Aug 30 23:14:02
Aug 30 23:29:18 localhost postfix/smtpd[12064]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:29:18
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:29:18
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max cache size 1 at Aug 30 23:29:18
Aug 30 23:44:50 localhost postfix/smtpd[12154]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:44:51 localhost postfix/smtpd[12154]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:44:51 localhost postfix/smtpd[12154]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:48:11 localhost postfix/anvil[12156]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:44:50
Aug 30 23:48:11 localhost postfix/anvil[12156]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:44:50
Aug 30 23:48:11 localhost postfix/anvil[12156]: statistics: max cache size 1 at Aug 30 23:44:50
Aug 31 00:00:22 localhost postfix/smtpd[15156]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 31 00:00:23 localhost postfix/smtpd[15156]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 31 00:00:23 localhost postfix/smtpd[15156]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 31 00:03:43 localhost postfix/anvil[15158]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 31 00:00:22

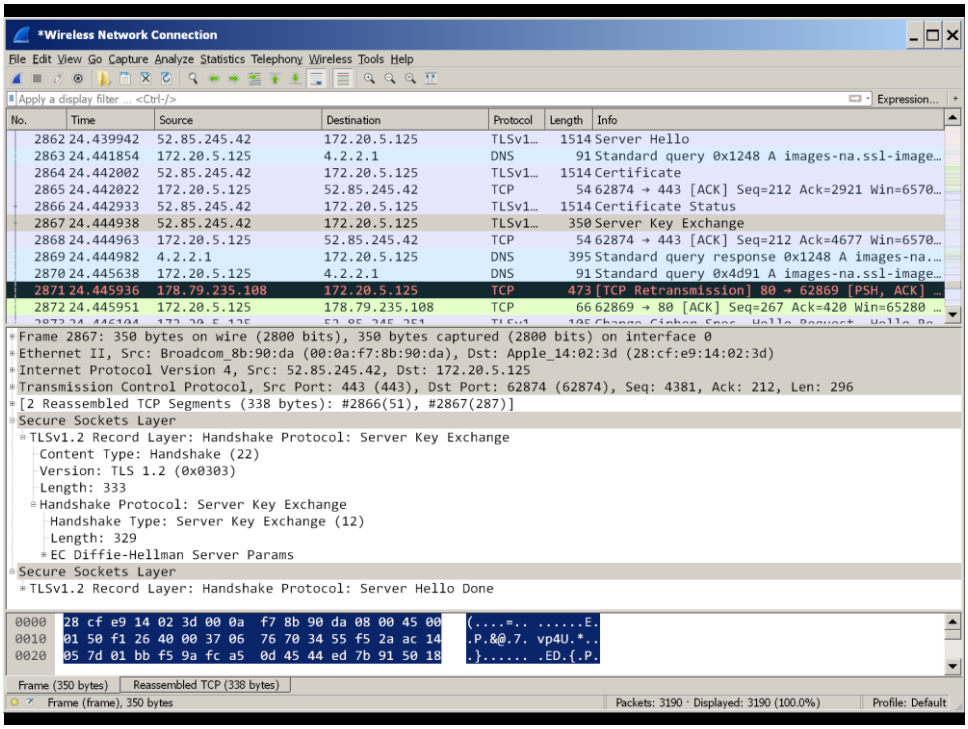

VIM
File Edit Tools Syntax Buffers Window Help
Aug 30 23:02:17 localhost postfix/anvil[11949]: statistics: max cache size 1 at Aug 30 22:58:56
Aug 30 23:14:02 localhost postfix/smtpd[12033]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max cache size 1 at Aug 30 23:14:02
Aug 30 23:29:18 localhost postfix/smtpd[12064]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:29:18
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:29:18
:set notitle
VIM
File Edit Tools Syntax Buffers Window Help
Introducing Windows 10
Your FREE Windows 10 upgrade is ready!
You're good to go!
Schedule your free upgrade!

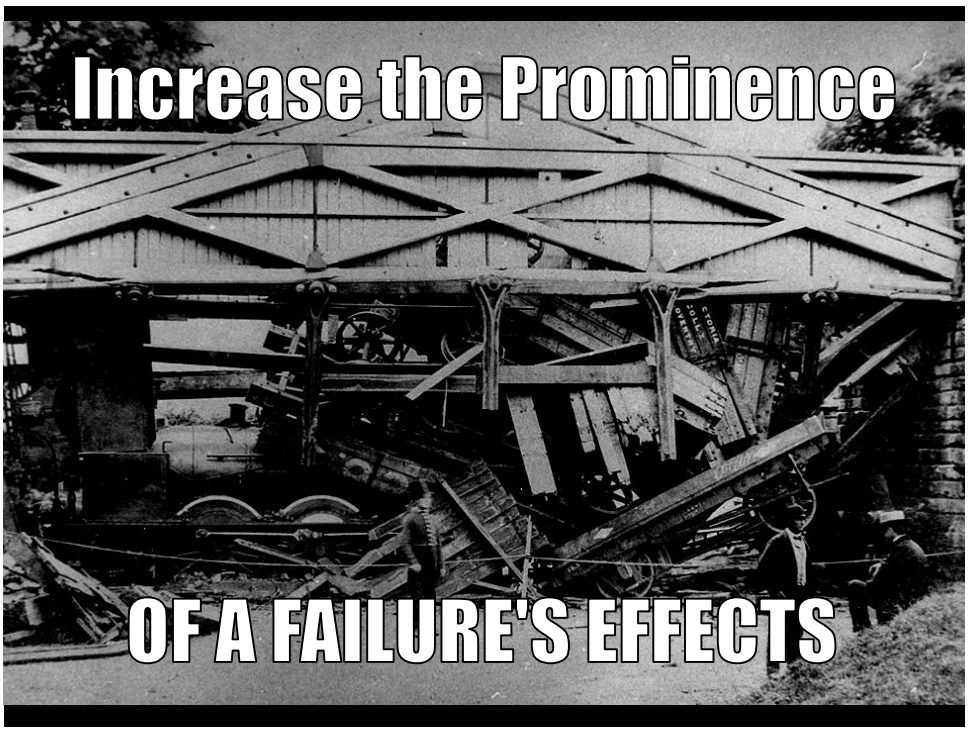

Consider Updating Your Software
Introducing Windows 10
Your FREE Windows 10 upgrade is ready!
You're good to go!
Schedule your free upgrade!

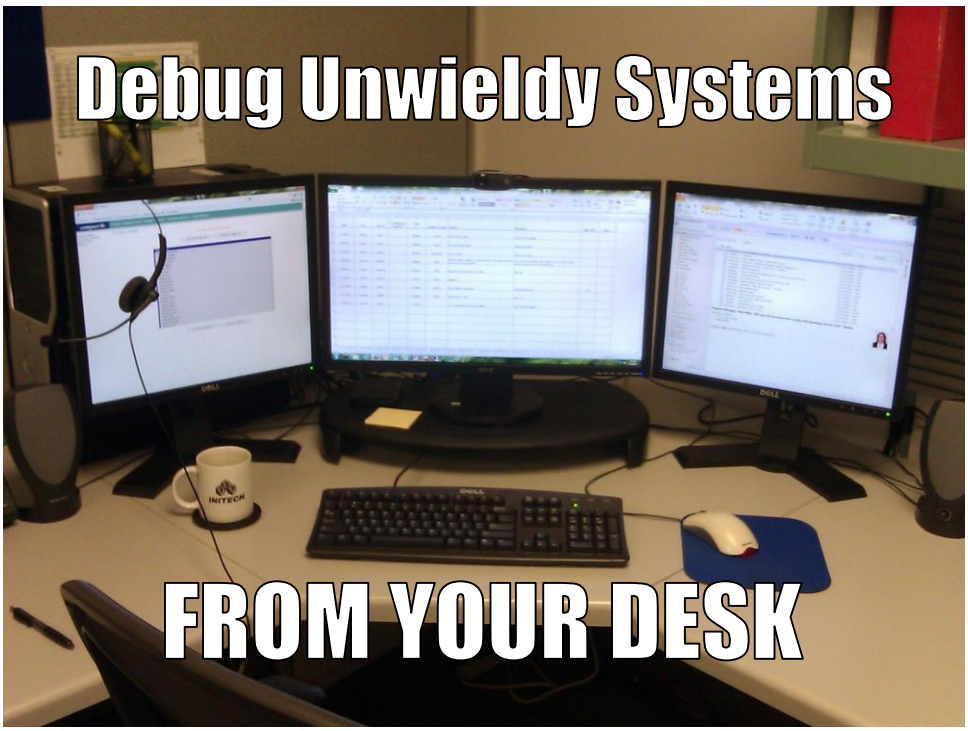

Use the Source Luke

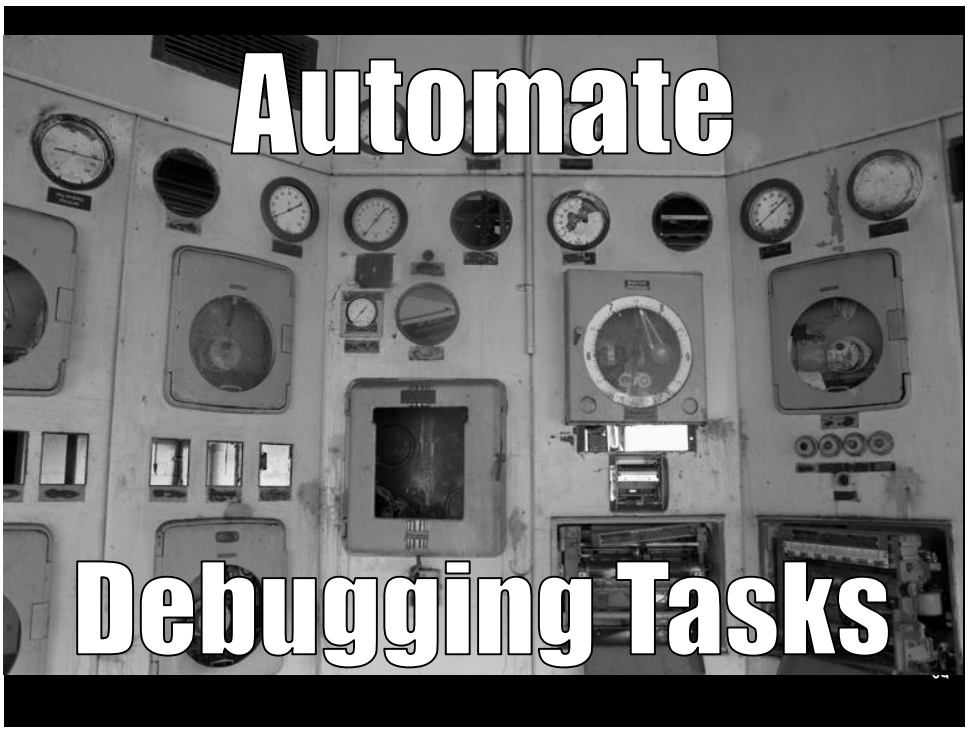
10Mbps Ethernet Hub

$139.99


*Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
2862 24.439942 52.85.245.42 172.20.5.125 TLSv1... 1514 Server Hello
2863 24.441854 172.20.5.125 4.2.2.1 DNS 91 Standard query 0x1248 A images-na.ssl-image...
2864 24.442002 52.85.245.42 172.20.5.125 TLSv1... 1514 Certificate
2865 24.442022 172.20.5.125 52.85.245.42 TCP 54 62874 → 443 [ACK] Seq=212 Ack=2921 Win=6570...
2866 24.442933 52.85.245.42 172.20.5.125 TLSv1... 1514 Certificate Status
2867 24.444938 52.85.245.42 172.20.5.125 TLSv1... 350 Server Key Exchange
2868 24.444963 172.20.5.125 52.85.245.42 TCP 54 62874 → 443 [ACK] Seq=212 Ack=4677 Win=6570...
2869 24.444982 4.2.2.1 172.20.5.125 DNS 395 Standard query response 0x1248 A images-na....
2870 24.445638 172.20.5.125 4.2.2.1 DNS 91 Standard query 0x4d91 A images-na.ssl-image...
2871 24.445936 178.79.235.108 172.20.5.125 TCP 473 [TCP Retransmission] 80 → 62869 [PSH, ACK] ...
2872 24.445951 172.20.5.125 178.79.235.108 TCP 66 62869 → 80 [ACK] Seq=267 Ack=420 Win=65280 ...
Frame 2867: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface 0
Ethernet II, Src: Broadcom_8b:90:da (00:0a:f7:8b:90:da), Dst: Apple_14:02:3d (28:cf:e9:14:02:3d)
Internet Protocol Version 4, Src: 52.85.245.42, Dst: 172.20.5.125
Transmission Control Protocol, Src Port: 443 (443), Dst Port: 62874 (62874), Seq: 4381, Ack: 212, Len: 296
[2 Reassembled TCP Segments (338 bytes): #2866(51), #2867(287)]
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 333
Handshake Protocol: Server Key Exchange
Handshake Type: Server Key Exchange (12)
Length: 329
EC Diffie-Hellman Server Params
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
0000 28 cf e9 14 02 3d 00 0a f7 8b 90 da 08 00 45 00 (....=.. ......E.
0010 01 50 f1 26 40 00 37 06 76 70 34 55 f5 2a ac 14 .P.&@.7. vp4U.*..
0020 05 7d 01 bb f5 9a fc a5 0d 45 44 ed 7b 91 50 18 .}...... .ED.{.P.
Frame (350 bytes)
Reassembled TCP (338 bytes)
Frame (frame), 350 bytes
Packets: 3190 · Displayed: 3190 (100.0%)
Profile: Default

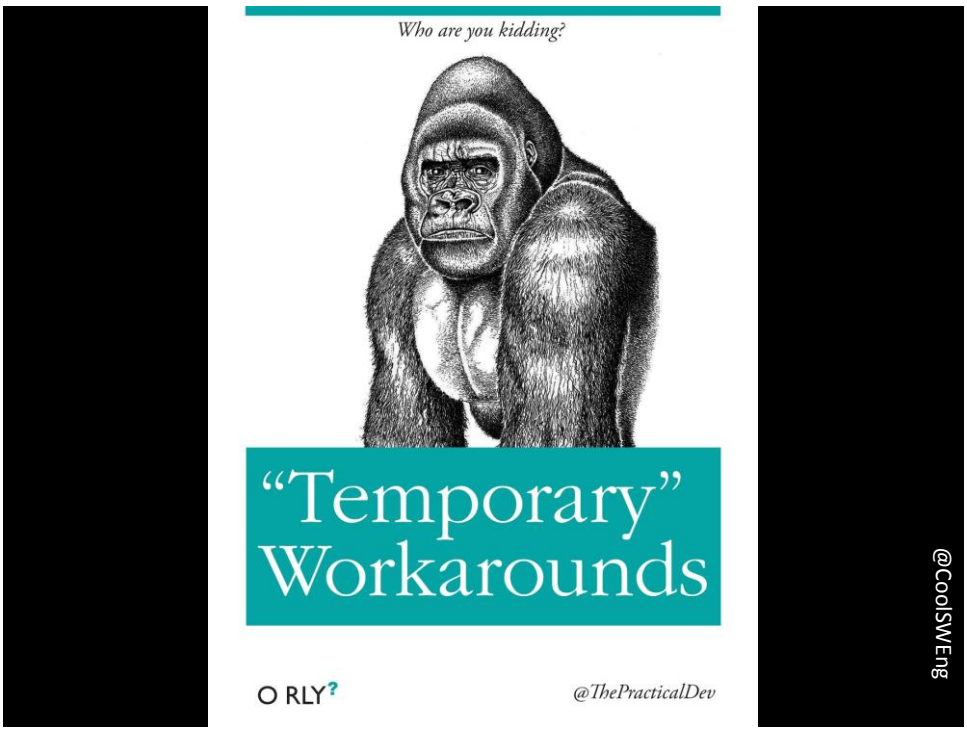

Increase the Prominence
OF A FAILURE'S EFFECTS


Debug Unwieldy Systems
FROM YOUR DESK


Automate
Debugging Tasks

```
# Obtain path
echo $PATH |
# Split the into lines
sed 's/:/\n/g' |
# For each line (path element)
while read path ; do
  # Time it
  PATH=$path:/usr/bin/time -f
"%e $path" which ls >/dev/null
done
```

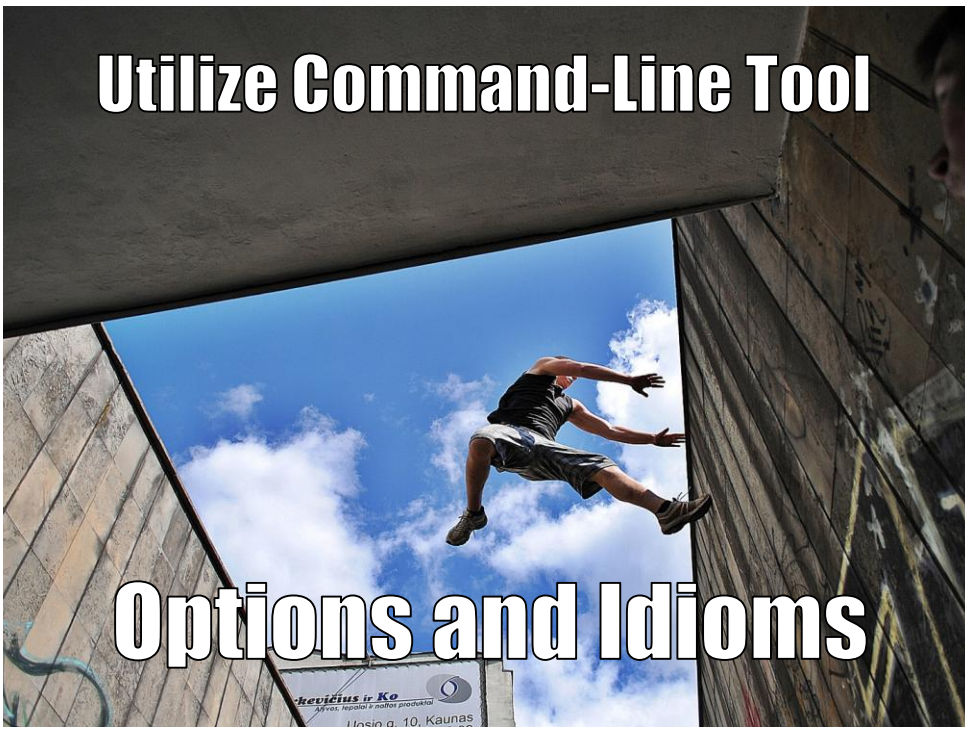
```
0.01 /usr/local/bin
0.01
/cygdrive/c/ProgramData/Oracle/Jav
a/javapath
0.01 /cygdrive/c/Python33
4.55 /
0.02 /cygdrive/c/usr/local/bin
0.01 /usr/bin
0.01 /cygdrive/c/usr/bin
0.01 /cygdrive/c/Windows/system32
0.01 /cygdrive/c/Windows
0.01 .
```


Who are you kidding?
"Temporary" Workarounds
O RLY?
@ThePracticalDev
@CoolSWEng


Fix All Instances
of a Problem Class


Tools & Techniques
GOT 'EM!

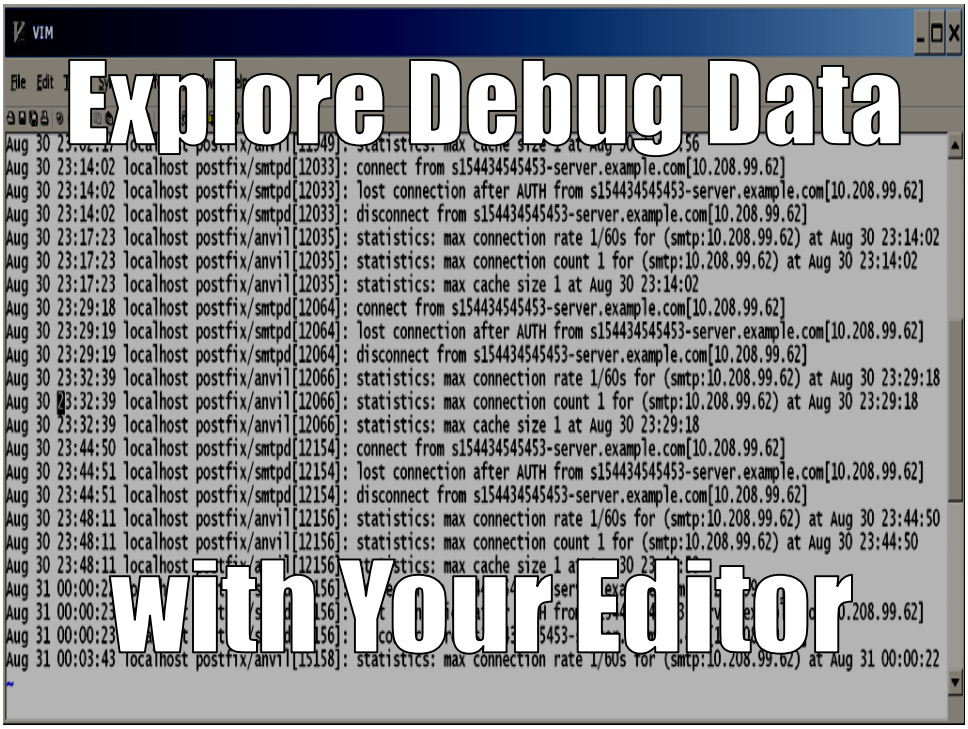

Unix Tools
Are Your Friends



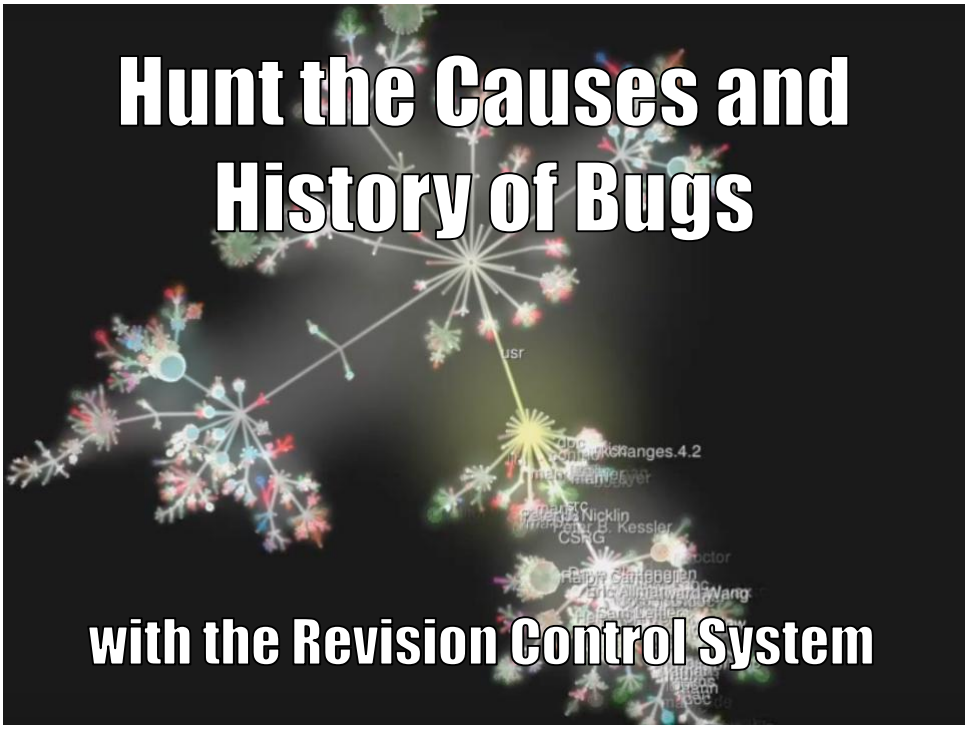

```
grep -r 'Dodgy doffset'

grep -r ' / ' . |
grep -v '/ sizeof'
```

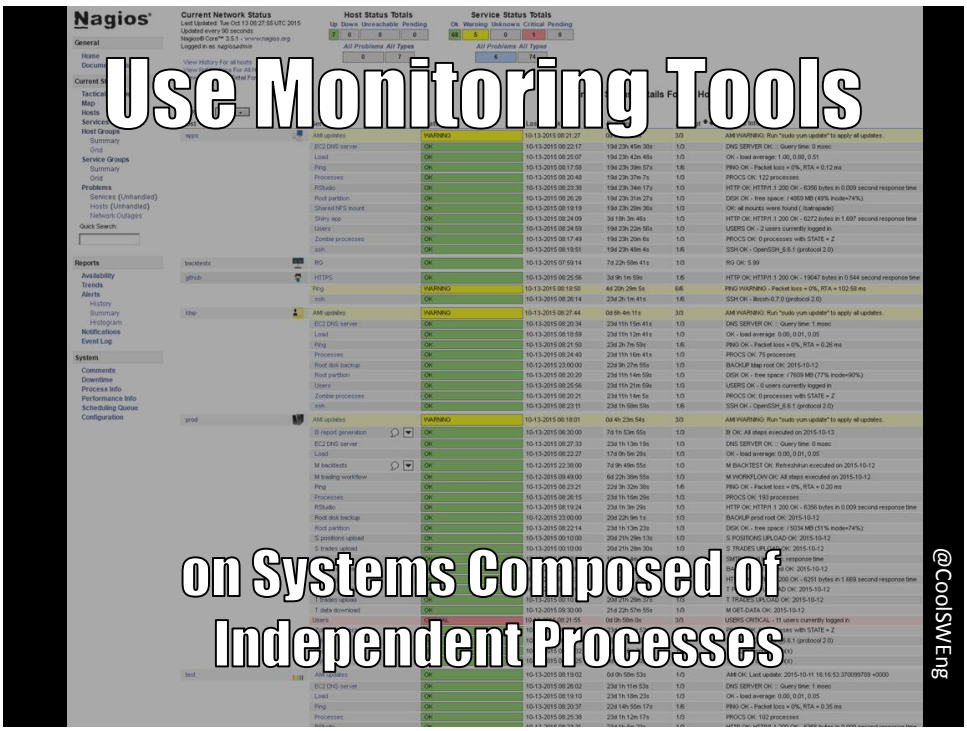
```
program 2>&1 | grep Fail
```

```
sudo tail –F /var/log/maillog

long-running-regression-test ; \
printf '\a'

sudo tail -F /var/log/secure |
fgrep -q 'Invalid user' ; \
printf '\a'

sudo tail -F /var/log/secure |
fgrep -m 1 'Invalid user' |
mail -s Intrusion jdh@example.com
```

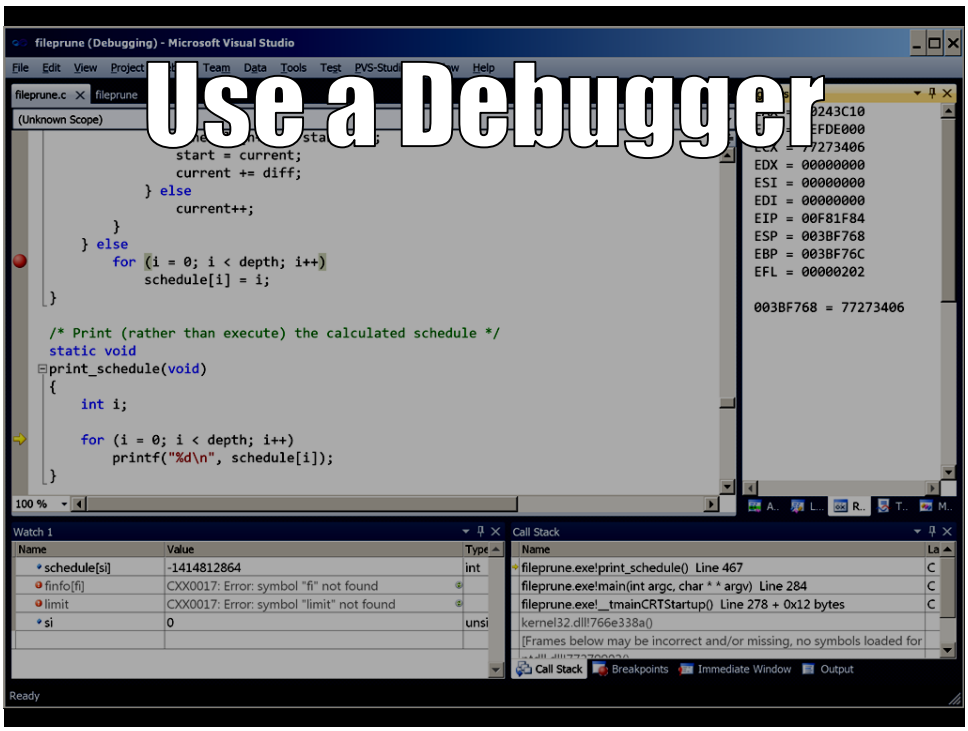

VIM
File Edit
Explore Debug Data
with Your Editor
Aug 30 23:14:02 localhost postfix/smtpd[12033]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:14:02 localhost postfix/smtpd[12033]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:14:02
Aug 30 23:17:23 localhost postfix/anvil[12035]: statistics: max cache size 1 at Aug 30 23:14:02
Aug 30 23:29:18 localhost postfix/smtpd[12064]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:29:19 localhost postfix/smtpd[12064]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:29:18
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:29:18
Aug 30 23:32:39 localhost postfix/anvil[12066]: statistics: max cache size 1 at Aug 30 23:29:18
Aug 30 23:44:50 localhost postfix/smtpd[12154]: connect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:44:51 localhost postfix/smtpd[12154]: lost connection after AUTH from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:44:51 localhost postfix/smtpd[12154]: disconnect from s154434545453-server.example.com[10.208.99.62]
Aug 30 23:48:11 localhost postfix/anvil[12156]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 30 23:44:50
Aug 30 23:48:11 localhost postfix/anvil[12156]: statistics: max connection count 1 for (smtp:10.208.99.62) at Aug 30 23:44:50
Aug 31 00:03:43 localhost postfix/anvil[15158]: statistics: max connection rate 1/60s for (smtp:10.208.99.62) at Aug 31 00:00:22

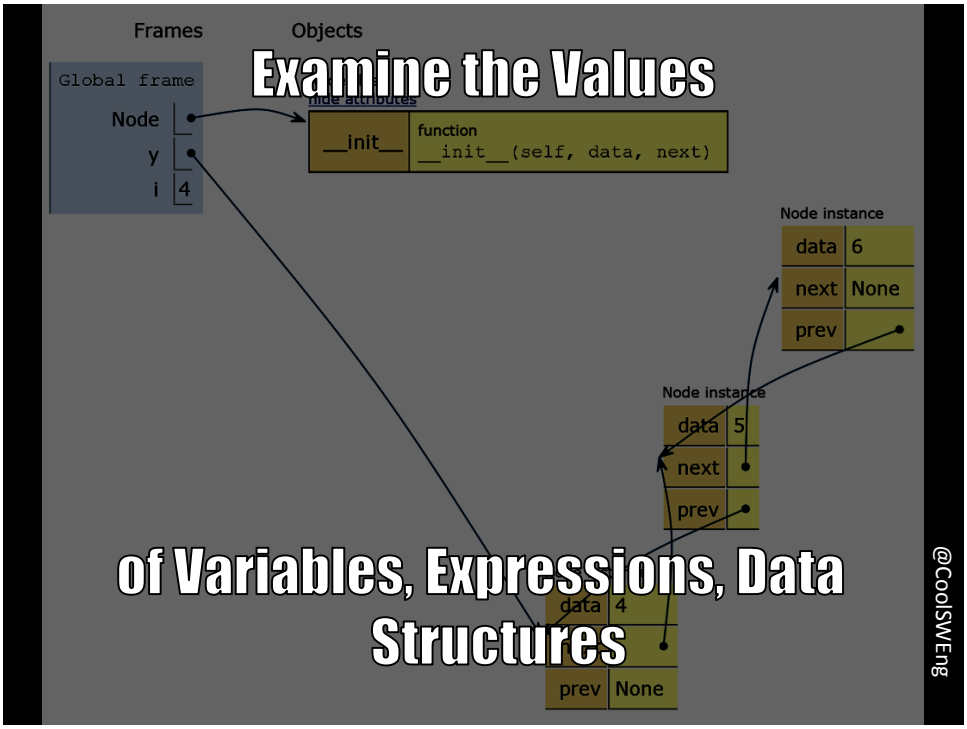

Optimize
Your Work Environment
PHP


Hunt the Causes and History of Bugs
with the Revision Control System

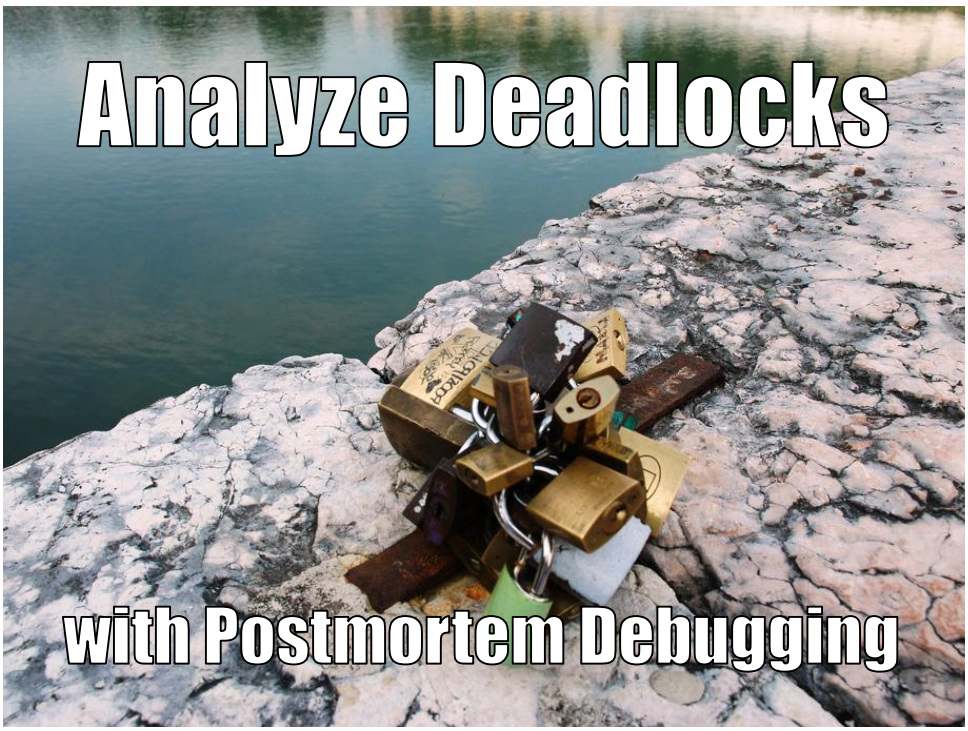

Use Monitoring Tools
on Systems Composed of Independent Processes
@CoolSWEng

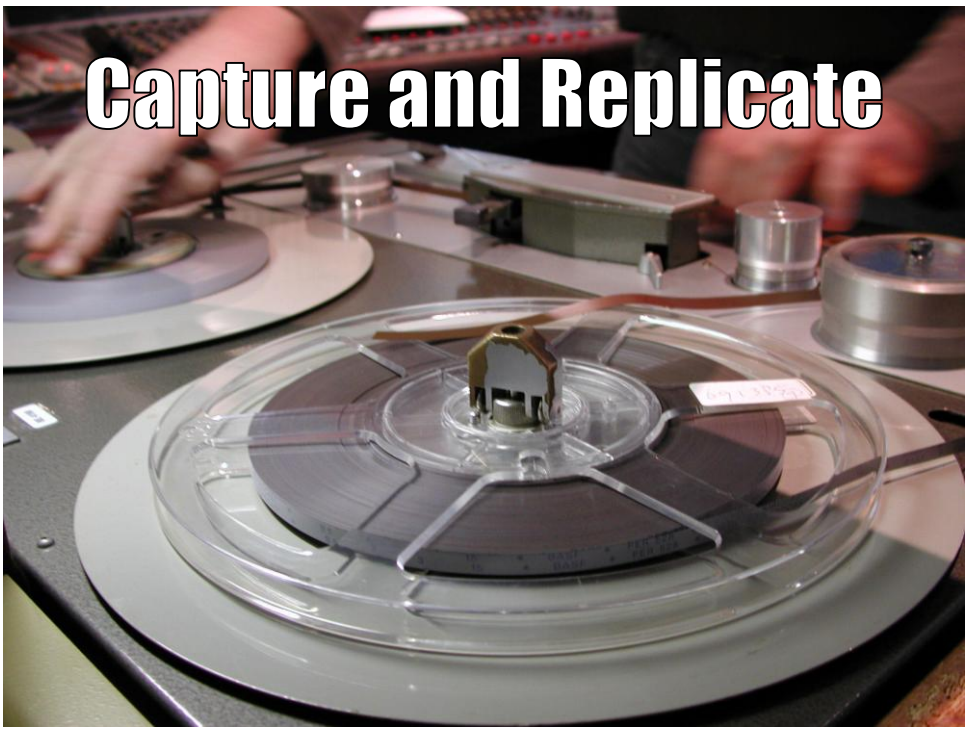

Debugger Techniques
GOT 'EM!


Use a Debugger
fileprune (Debugging) - Microsoft Visual Studio
File Edit View Project Team Data Tools Test PVS-Studio Window Help
fileprune.c
fileprune
(Unknown Scope)
start = current;
current += diff;
} else
current++;
}
} else
for (i = 0; i < depth; i++)
schedule[i] = i;
}
/* Print (rather than execute) the calculated schedule */
static void
print_schedule(void)
{
int i;
for (i = 0; i < depth; i++)
printf("%d\n", schedule[i]);
}
EDX = 00000000
ESI = 00000000
EDI = 00000000
EIP = 00F81F84
ESP = 003BF768
EBP = 003BF76C
EFL = 00000202
003BF768 = 77273406
100 %
Watch 1
Name
Value
Type
schedule[si]
-1414812864
int
finfo[fi]
CXX0017: Error: symbol "fi" not found
limit
CXX0017: Error: symbol "limit" not found
si
0
unsi
Call Stack
Name
fileprune.exe!print_schedule() Line 467
fileprune.exe!main(int argc, char * * argv) Line 284
fileprune.exe!__tmainCRTStartup() Line 278 + 0x12 bytes
kernel32.dll!766e338a()
[Frames below may be incorrect and/or missing, no symbols loaded for
Call Stack
Breakpoints
Immediate Window
Output
Ready



"When two trains approach each other at a crossing, both shall come to a full stop and neither shall start up again until the other has gone."


Analyze Deadlocks
with Postmortem Debugging

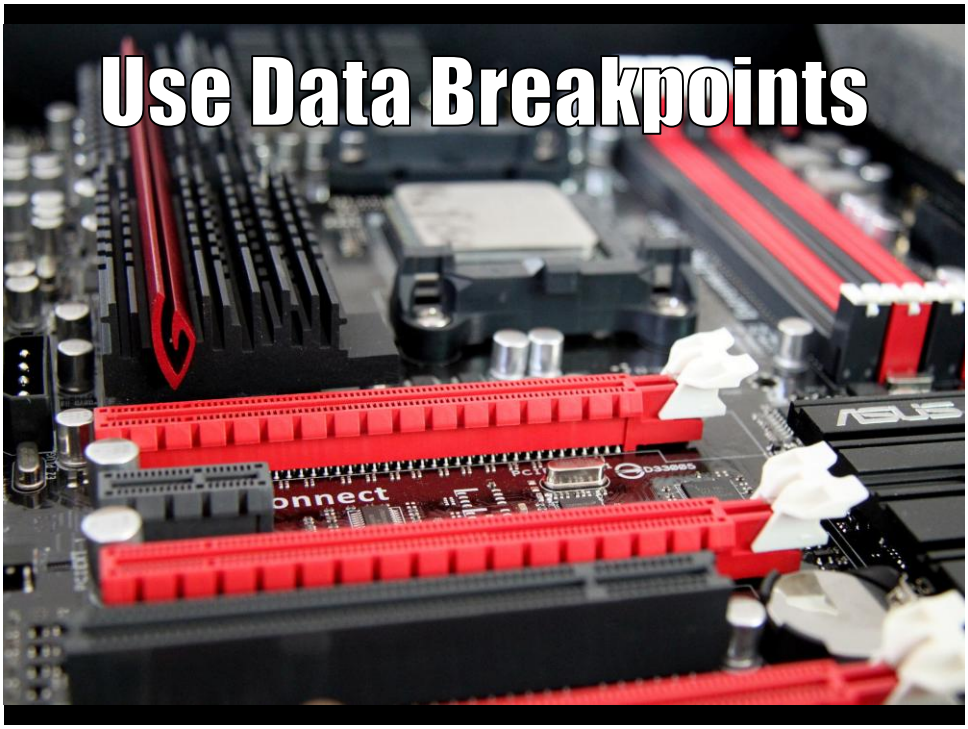

Capture and Replicate

```
$ ./race
counter=100000
$ ./race
counter=103754
$ ./race
counter=101233
$ ./race
counter=100000
$ ./race
counter=103977
```

```
$ gdb_record race
(gdb) break main
Breakpoint 1 at 0x400730: file race.c, line 28.
(gdb) continue
Continuing.
Breakpoint 1, main () at race.c:28
28          for (i = 0; i < 2; i++)
(gdb) pin record on
monitor record on
Started recording region number 0
(gdb) continue
Continuing.
counter=127873
[Inferior 1 (Remote target) exited normally]
(gdb) quit
```

```
$ replay pinball/log_0
counter=127873
$ replay pinball/log_0
counter=127873
$ replay pinball/log_0
counter=127873
```

```
$ gdb_replay pinball/log_0 ./race
0x0000000000400737 in main () at race.c:28
28          for (i = 0; i < 2; i++)
(gdb) pin break 16 if tmp == 0x108e5
monitor break at 0x4006fe if [ 0x4006ed : %rsp + -12 ]
4 == 0x108e5 #tmp:<16>
```

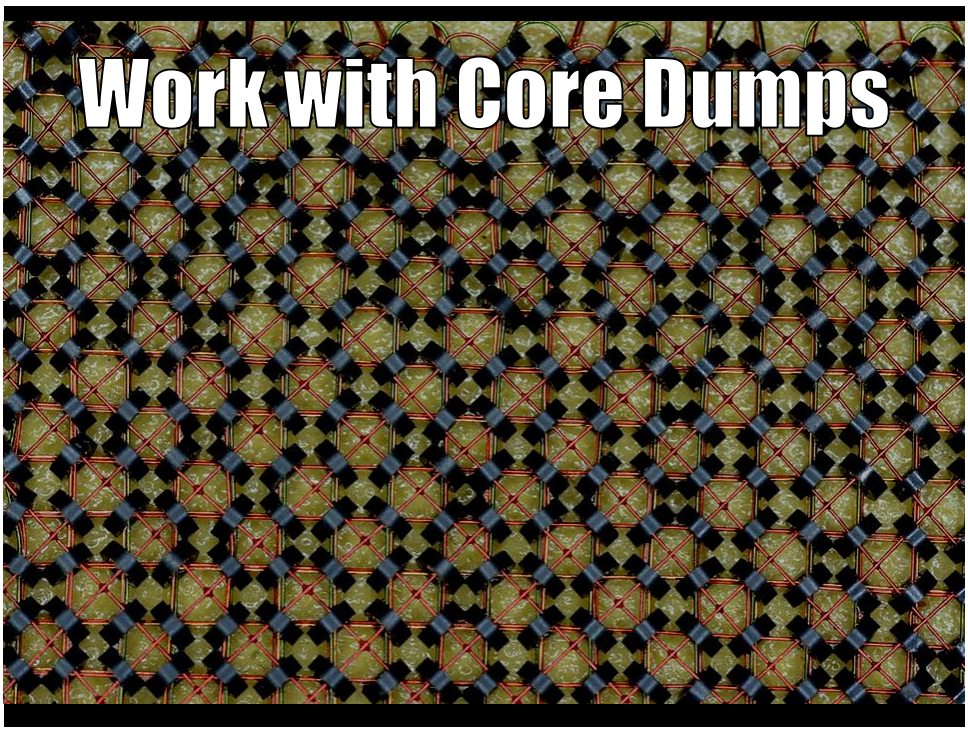

Use Data Breakpoints

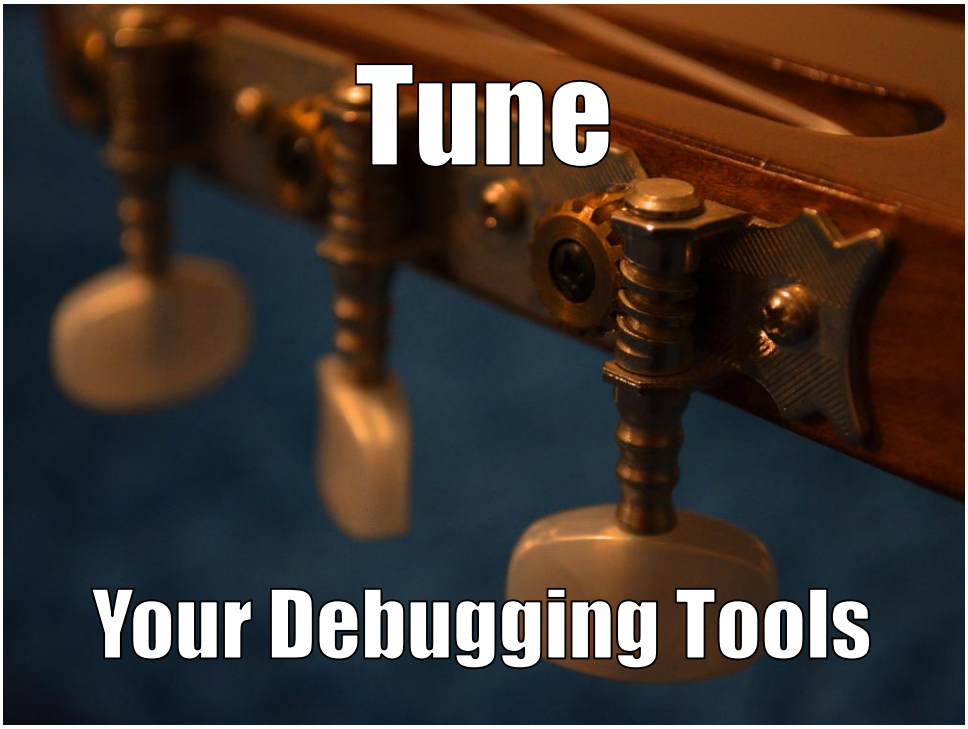

Reverse
Debugging
@CoolSWEng

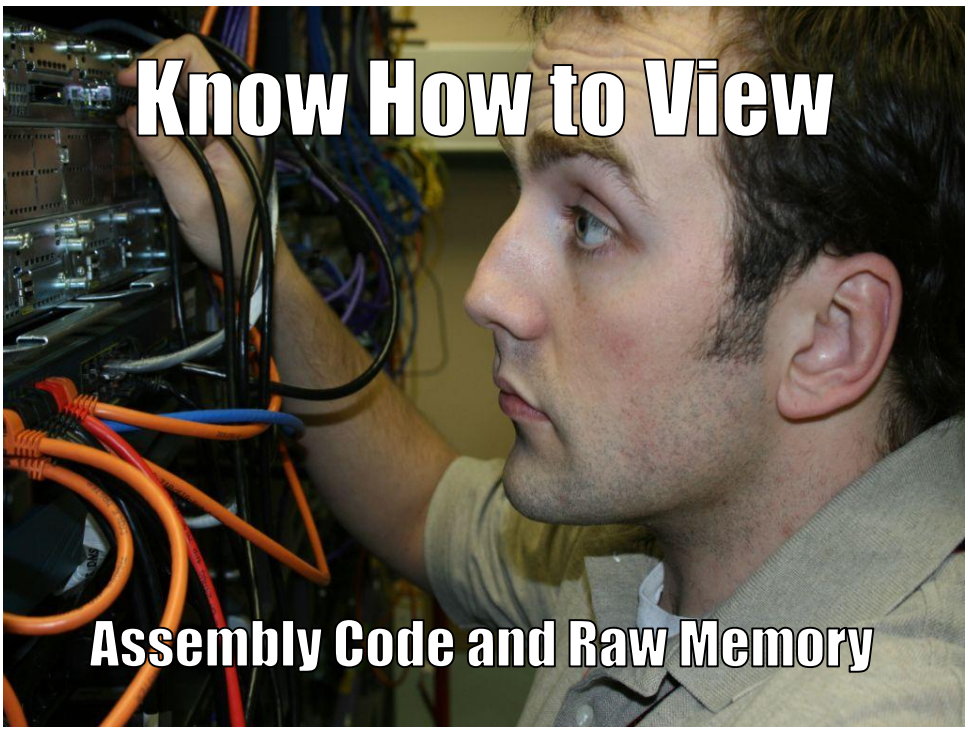
```
(gdb) display i
(gdb) display sum
(gdb) break 10
Breakpoint 2 at 0x400542: file loop.c, line 10.
(gdb) record
(gdb) cont
Continuing.
45
Breakpoint 2, main () at loop.c:10
10    }
2: sum = 45
1: i = 10
```

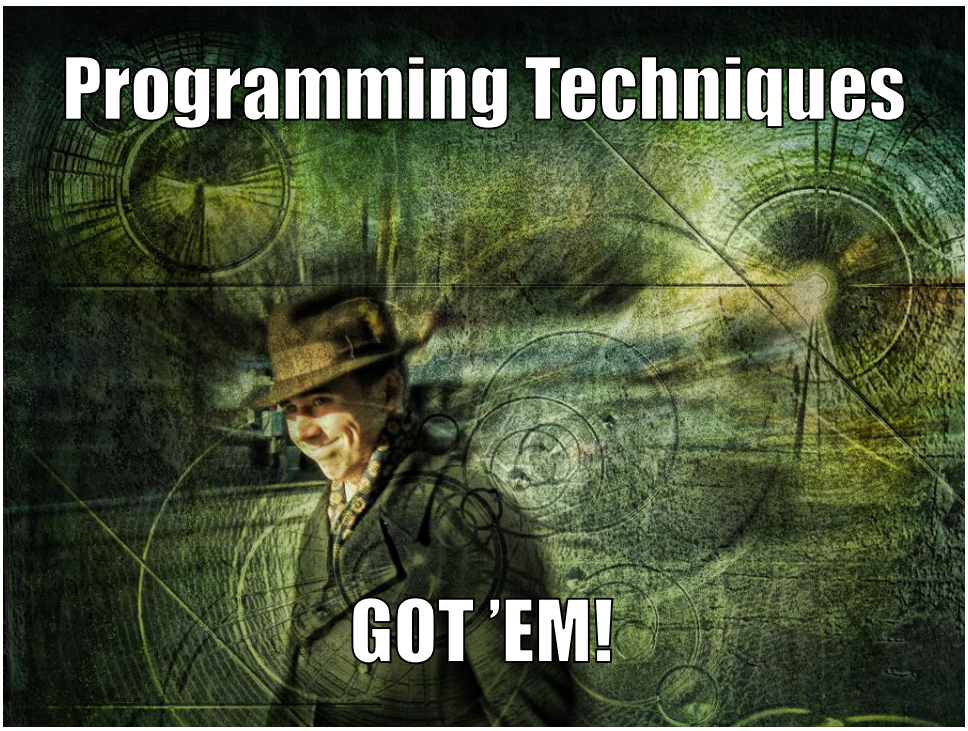
```
(gdb) reverse-next
9           printf("%d\n", sum);
2: sum = 45
1: i = 10
(gdb) reverse-next
7           for (i = 0; i < 10; i++)
2: sum = 45
1: i = 9
(gdb) reverse-next
8                   sum += i;
2: sum = 36
1: i = 9
```

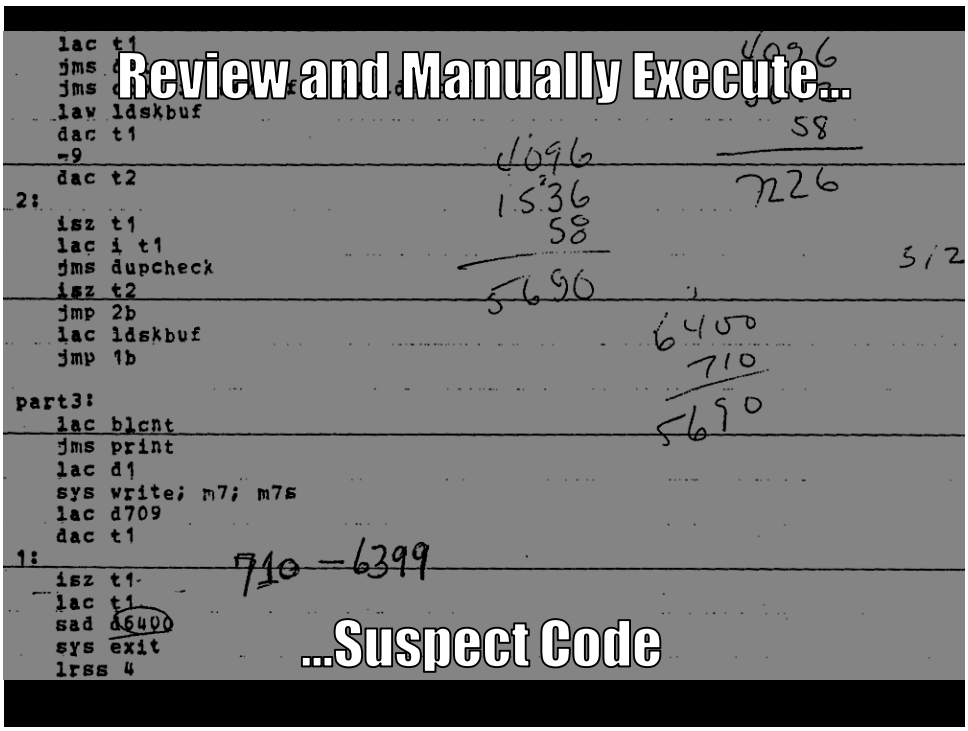

Attach a Debugger
to a Running Process

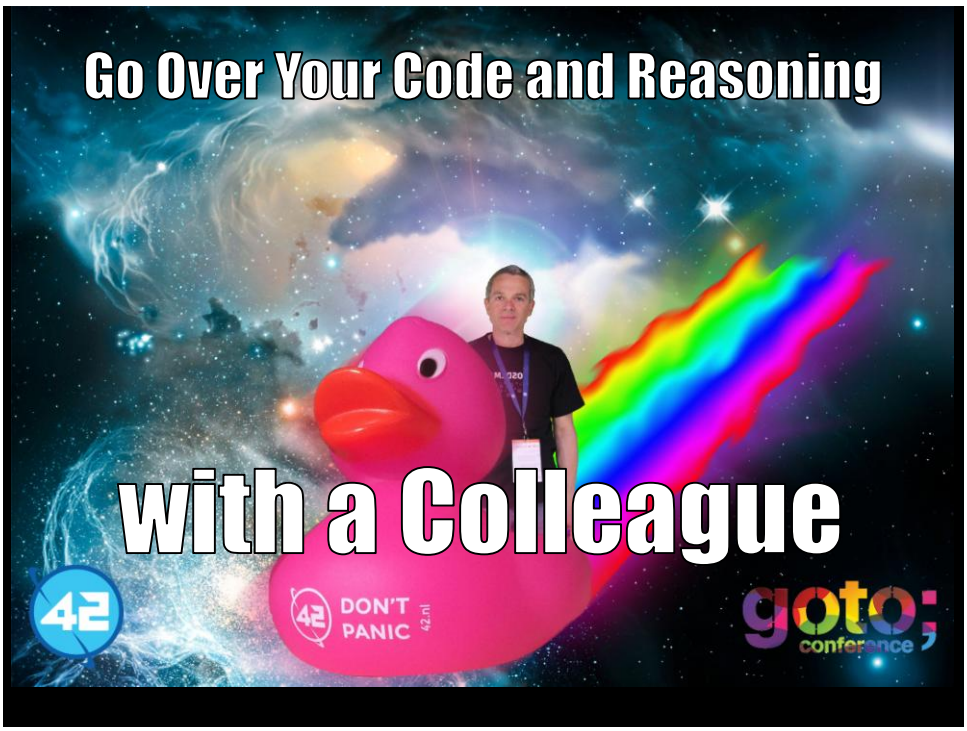

Work with Core Dumps


Tune
Your Debugging Tools

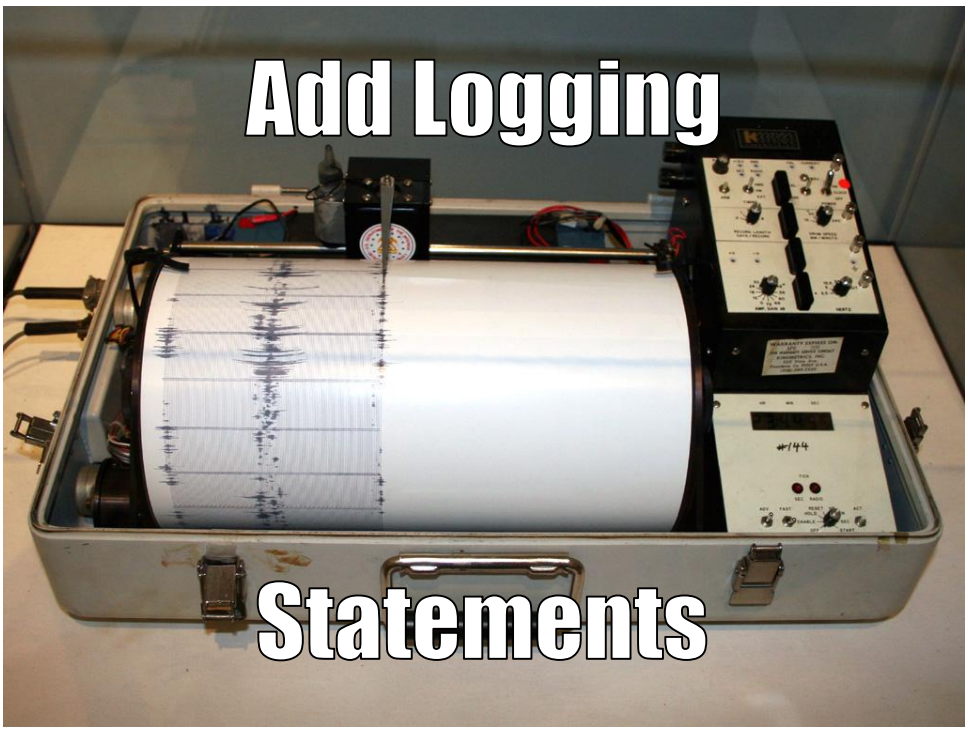

Know How to View
Assembly Code and Raw Memory

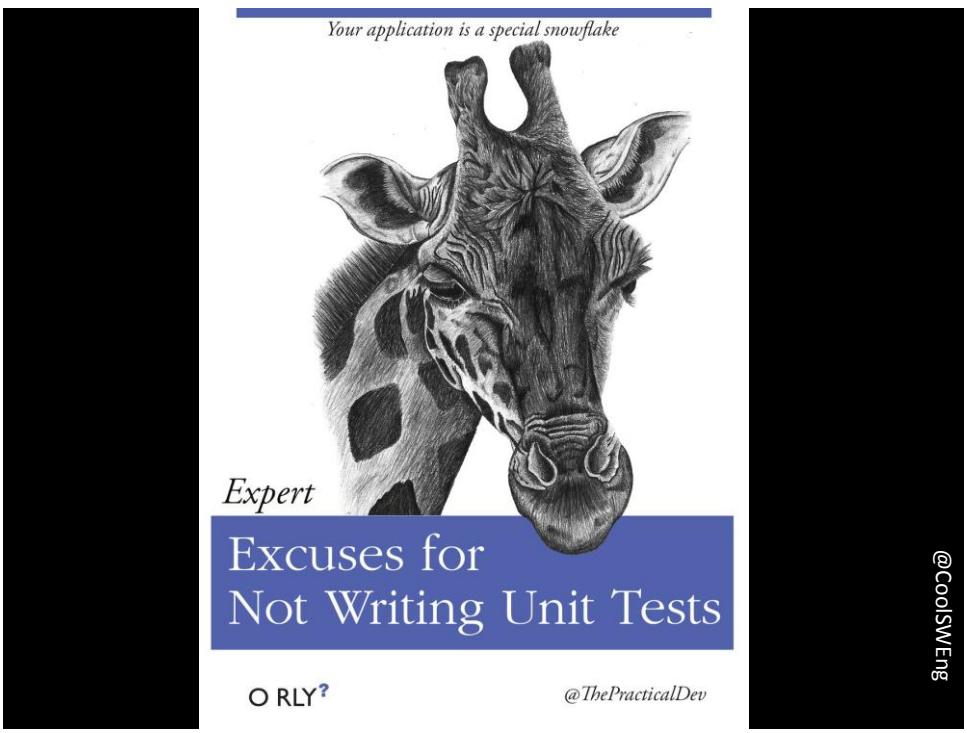

Programming Techniques
GOT 'EM!


Review and Manually Execute...
...Suspect Code
lac t1
jms
jms
law ldskbuf
dac t1
-9
dac t2
2:
isz t1
lac i t1
jms dupcheck
isz t2
jmp 2b
lac ldskbuf
jmp 1b
part3:
lac blcnt
jms print
lac d1
sys write; m7; m7s
lac d709
dac t1
1:
isz t1
lac t1
sad d6400
sys exit
lrss 4


Go Over Your Code and Reasoning
with a Colleague
42
DON'T PANIC
42.nl
goto;
conference

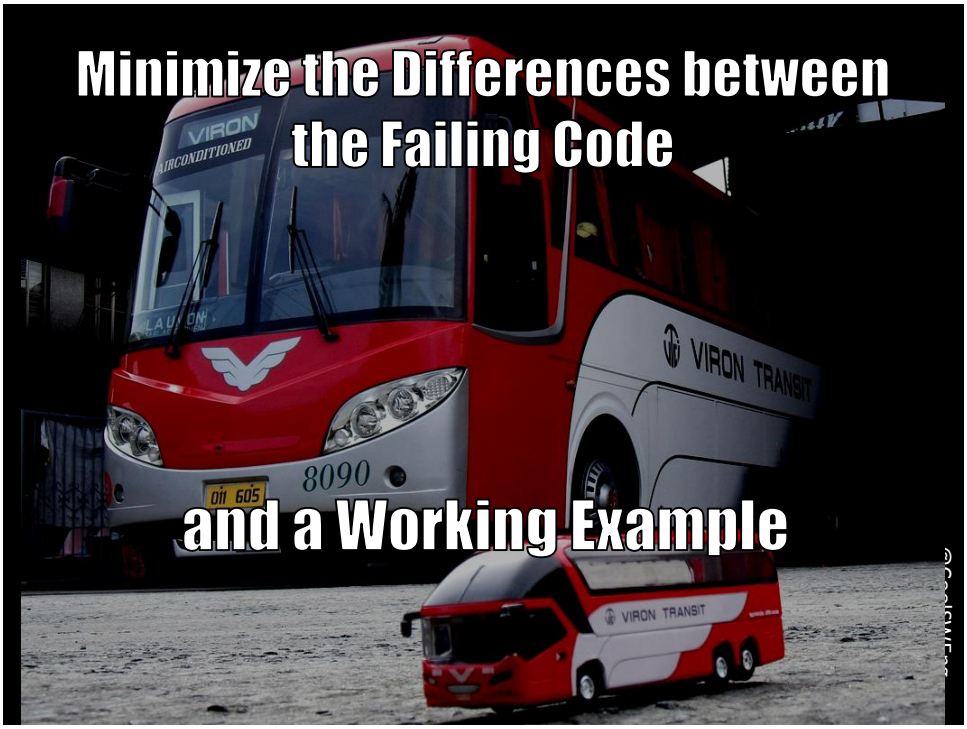

Add Debugging Functionality

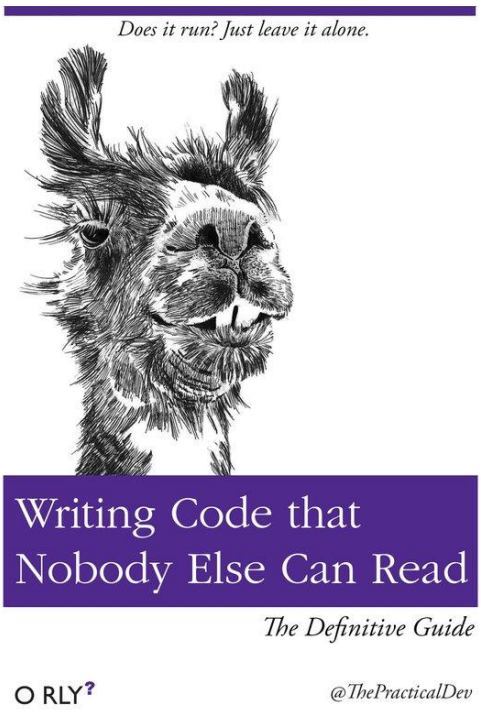

Add Logging
Statements


Your application is a special snowflake
Expert
Excuses for
Not Writing Unit Tests
O RLY?
@ThePracticalDev
@CoolSWEng

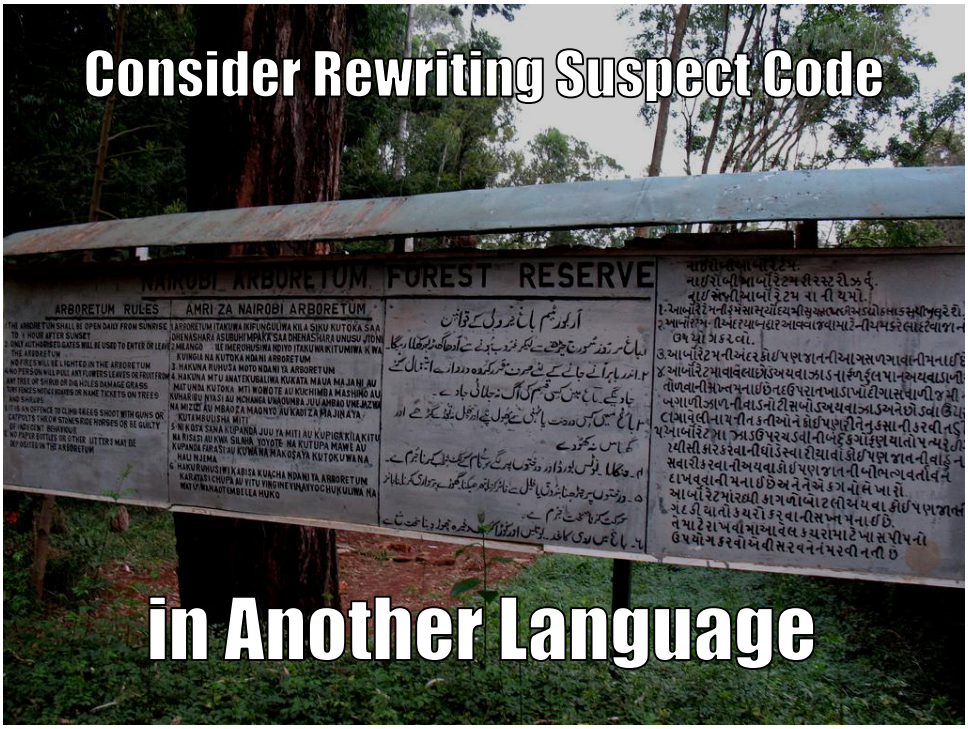

Use Assertions

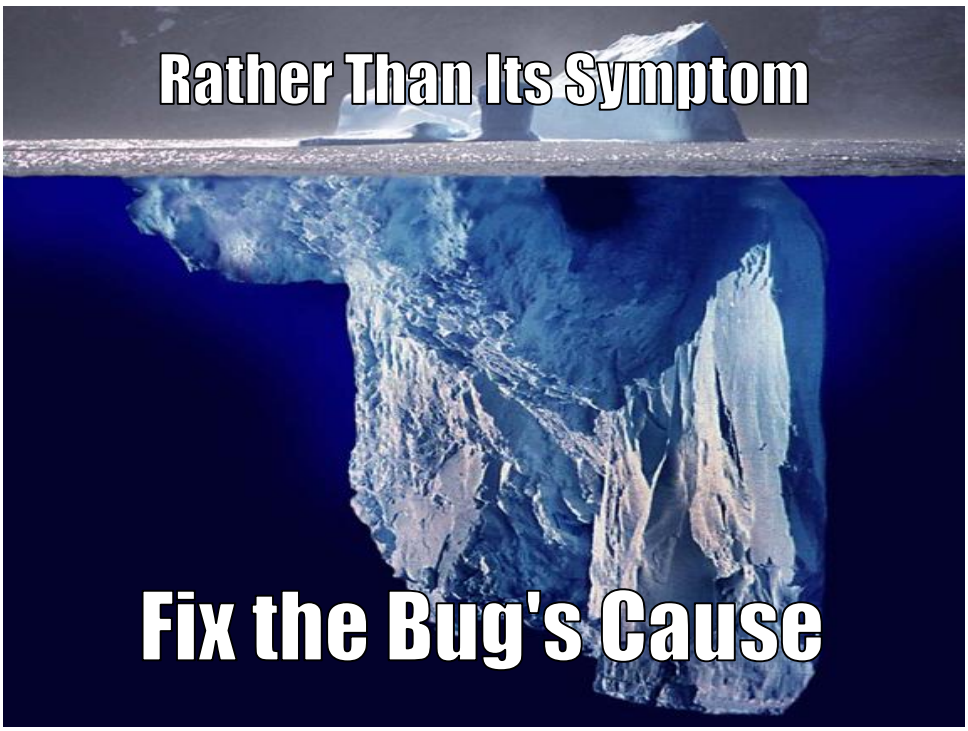

Verify Your Reasoning
by Perturbing
the Debugged Program


Minimize the Differences between the Failing Code
and a Working Example
VIRON
AIRCONDITIONED
VIRON TRANSIT
8090
VIRON TRANSIT

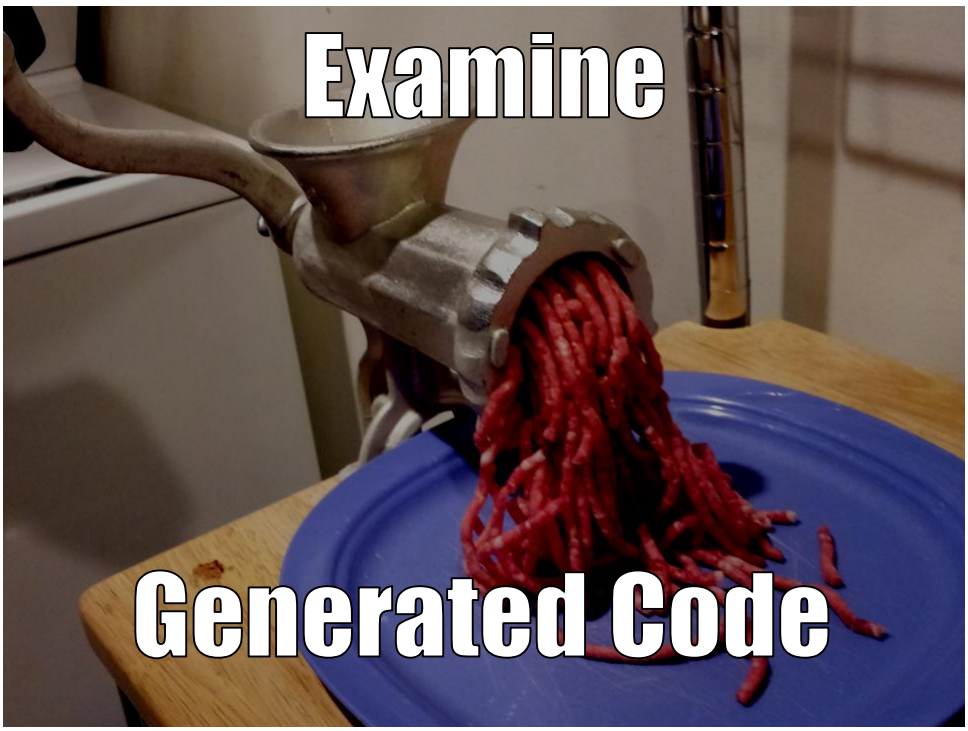

Does it run? Just leave it alone.
Writing Code that Nobody Else Can Read
The Definitive Guide
O RLY?
@ThePracticalDev

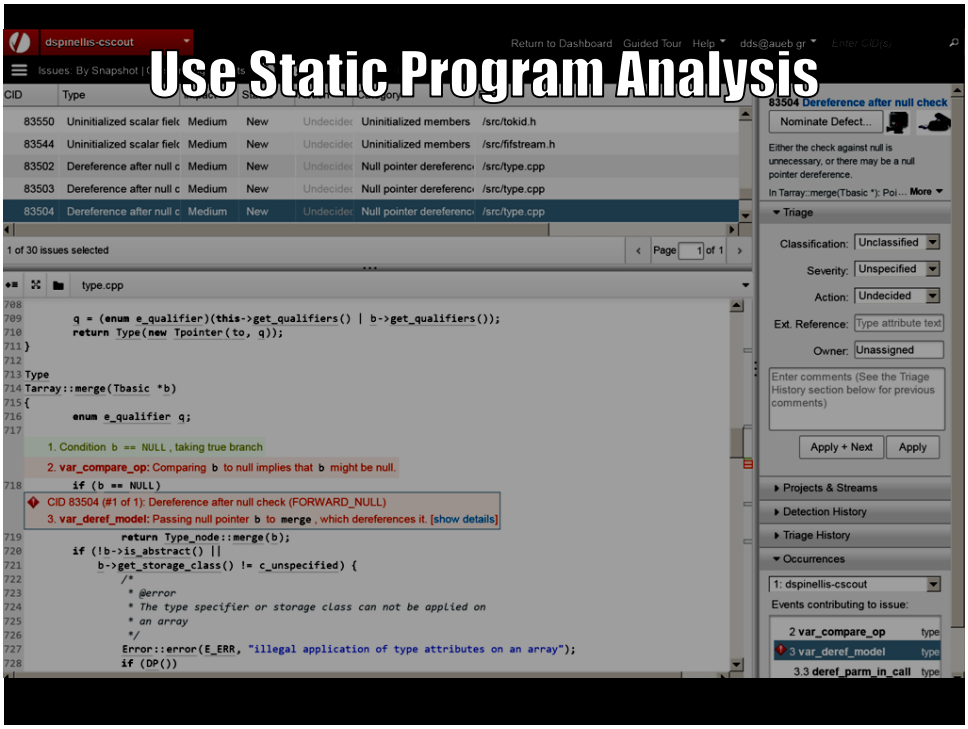
@CoolSWEng


Consider Rewriting Suspect Code
NAIROBI ARBORETUM FOREST RESERVE
ARBORETUM RULES
AMRI ZA NAIROBI ARBORETUM
in Another Language

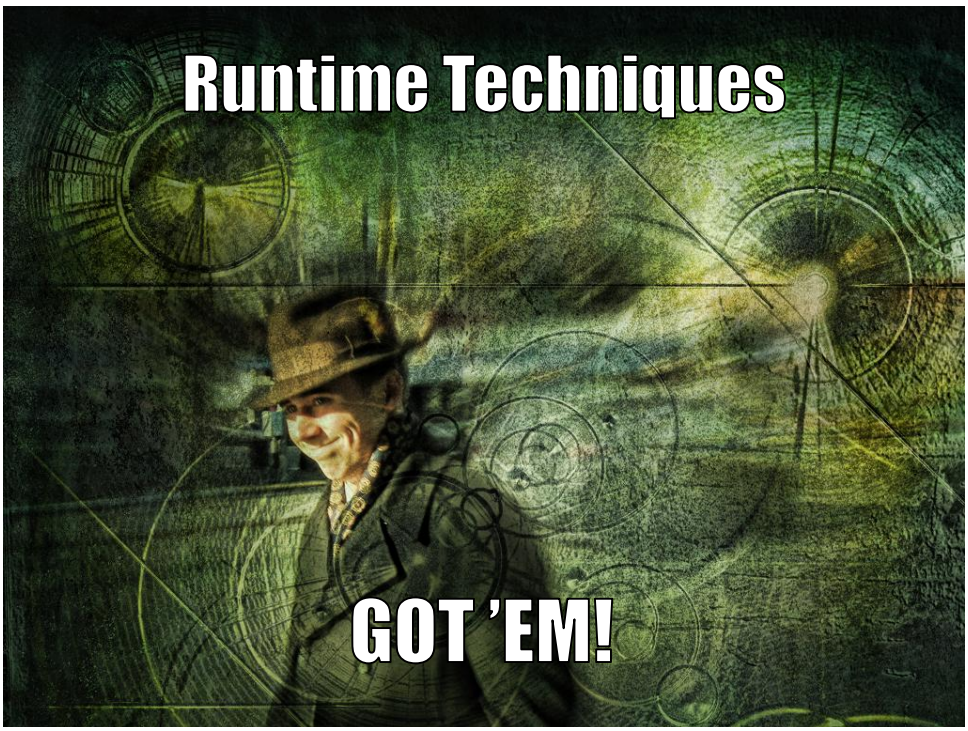

Rather Than Its Symptom
Fix the Bug's Cause

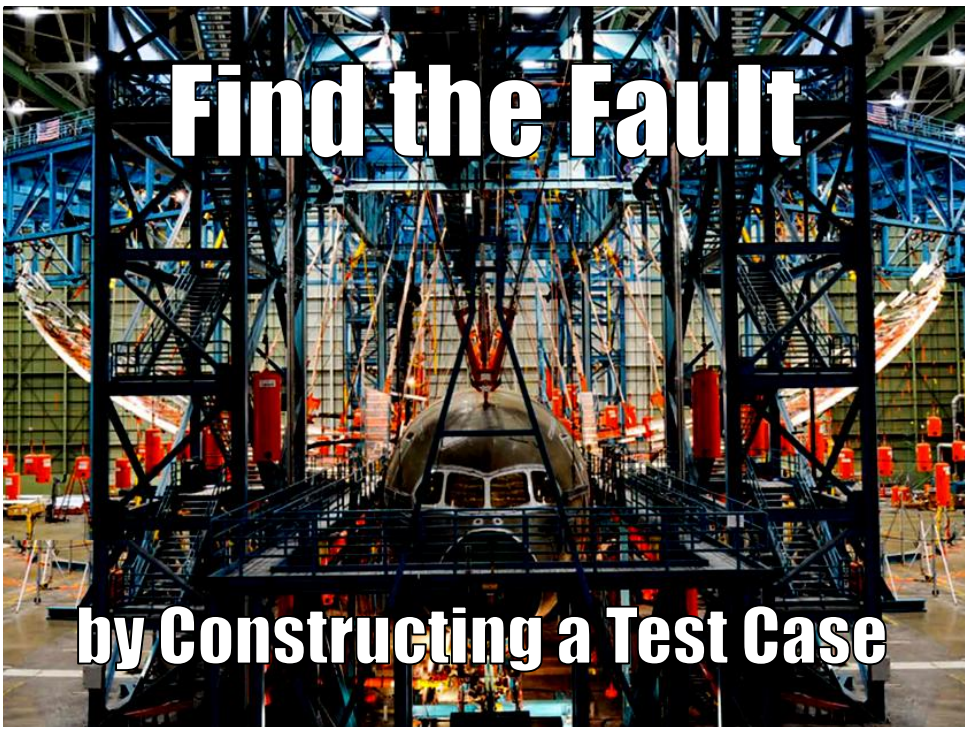

Compile-Time Techniques
GOT 'EM!

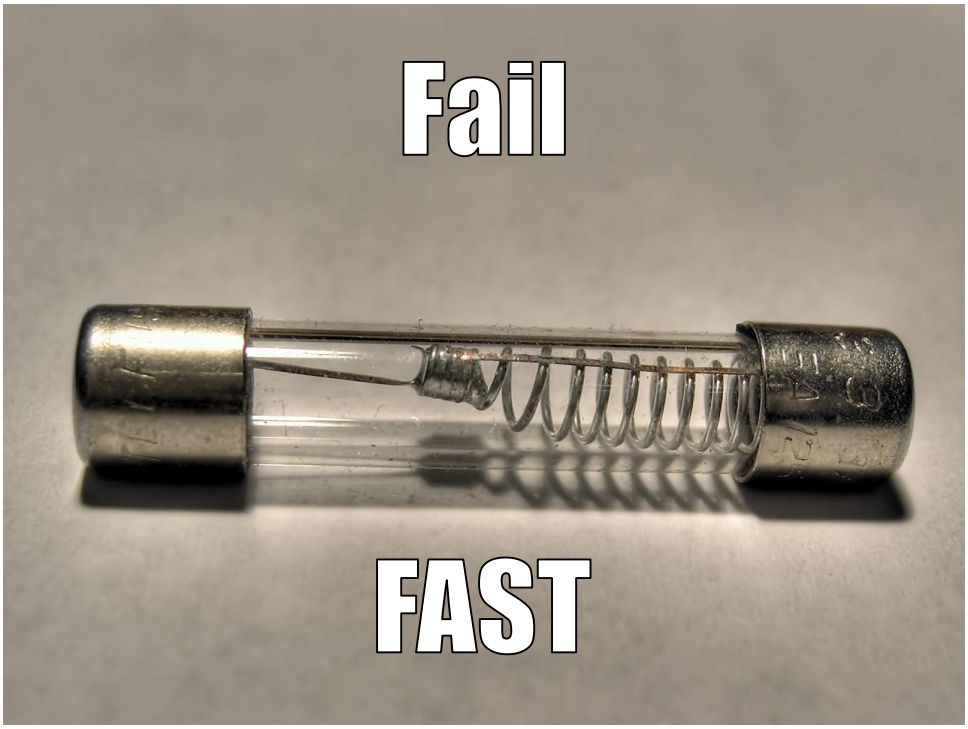

Examine
Generated Code

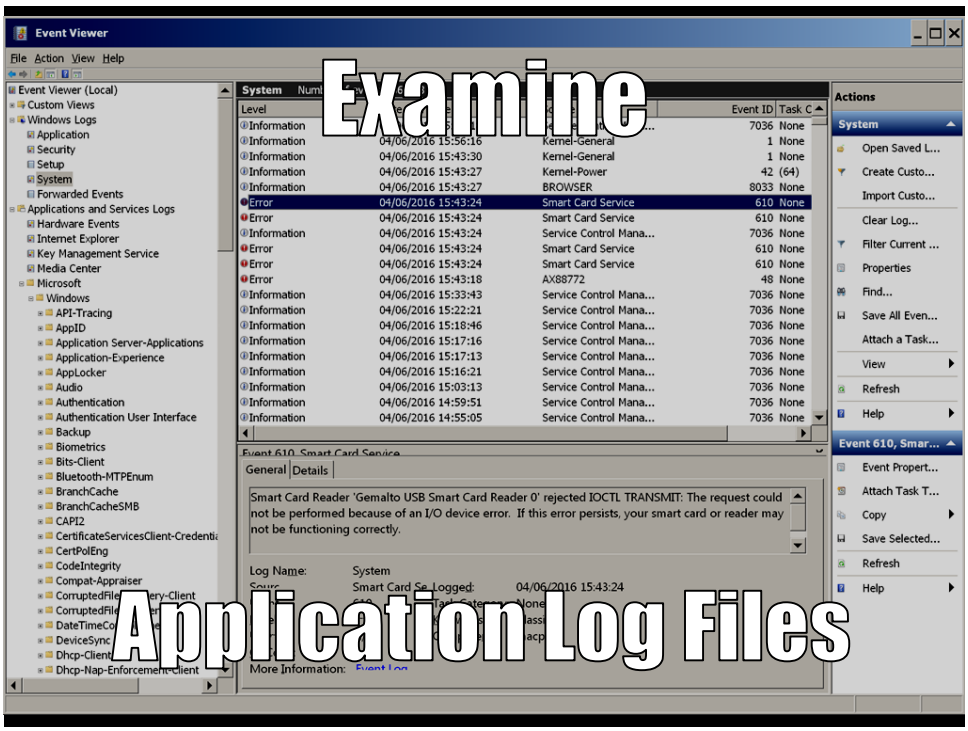

Use Static Program Analysis
dspinellis-cscout
Return to Dashboard
Guided Tour
Help
dds@aueb.gr
Issues: By Snapshot
CID
Type
83550 Uninitialized scalar fiel Medium New Uninitialized members /src/tokid.h
83544 Uninitialized scalar fiel Medium New Uninitialized members /src/fifstream.h
83502 Dereference after null c Medium New Null pointer dereferenc /src/type.cpp
83503 Dereference after null c Medium New Null pointer dereferenc /src/type.cpp
83504 Dereference after null c Medium New Null pointer dereferenc /src/type.cpp
1 of 30 issues selected
Page 1 of 1
type.cpp
q = (enum e_qualifier)(this->get_qualifiers() | b->get_qualifiers());
return Type(new Tpointer(to, q));
}
Type
Tarray::merge(Tbasic *b)
{
enum e_qualifier q;
1. Condition b == NULL, taking true branch
2. var_compare_op: Comparing b to null implies that b might be null.
if (b == NULL)
CID 83504 (#1 of 1): Dereference after null check (FORWARD_NULL)
3. var_deref_model: Passing null pointer b to merge, which dereferences it. [show details]
return Type_node::merge(b);
if (!b->is_abstract() ||
b->get_storage_class() != c_unspecified) {
/*
* @error
* The type specifier or storage class can not be applied on
* an array
*/
Error::error(E_ERR, "illegal application of type attributes on an array");
if (DP())
83504 Dereference after null check
Nominate Defect...
Either the check against null is unnecessary, or there may be a null pointer dereference.
In Tarray::merge(Tbasic *): Poi... More
Triage
Classification: Unclassified
Severity: Unspecified
Action: Undecided
Ext. Reference: Type attribute text
Owner: Unassigned
Enter comments (See the Triage History section below for previous comments)
Apply + Next
Apply
Projects & Streams
Detection History
Triage History
Occurrences
1: dspinellis-cscout
Events contributing to issue:
2 var_compare_op type
3 var_deref_model type
3.3 deref_parm_in_call type

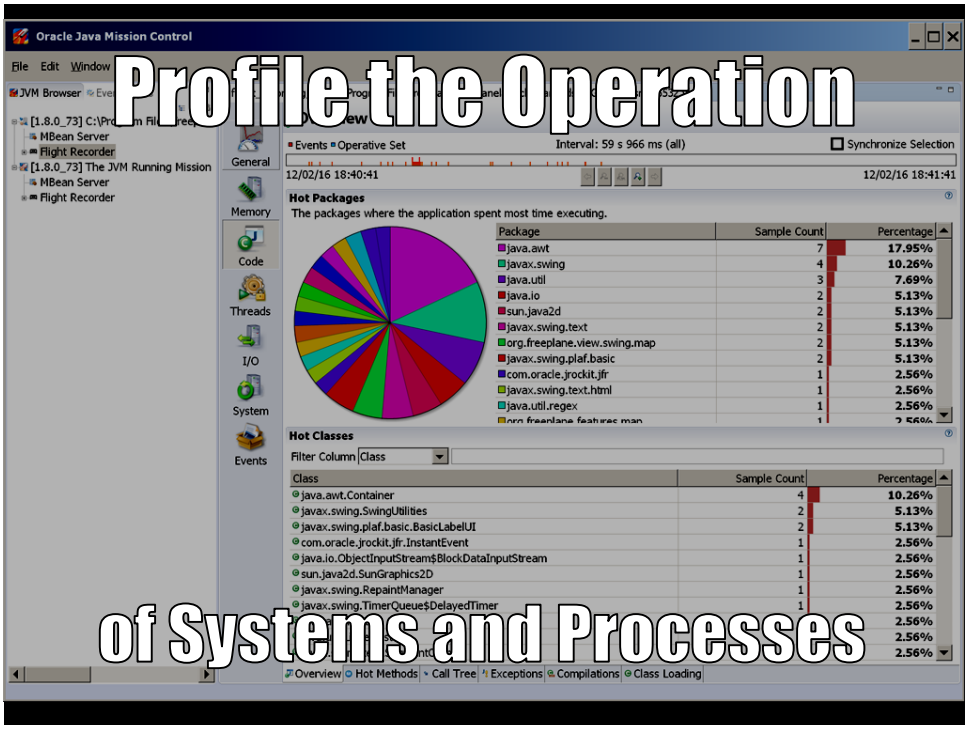

Configure the Use of
Debugging Libraries and Checks

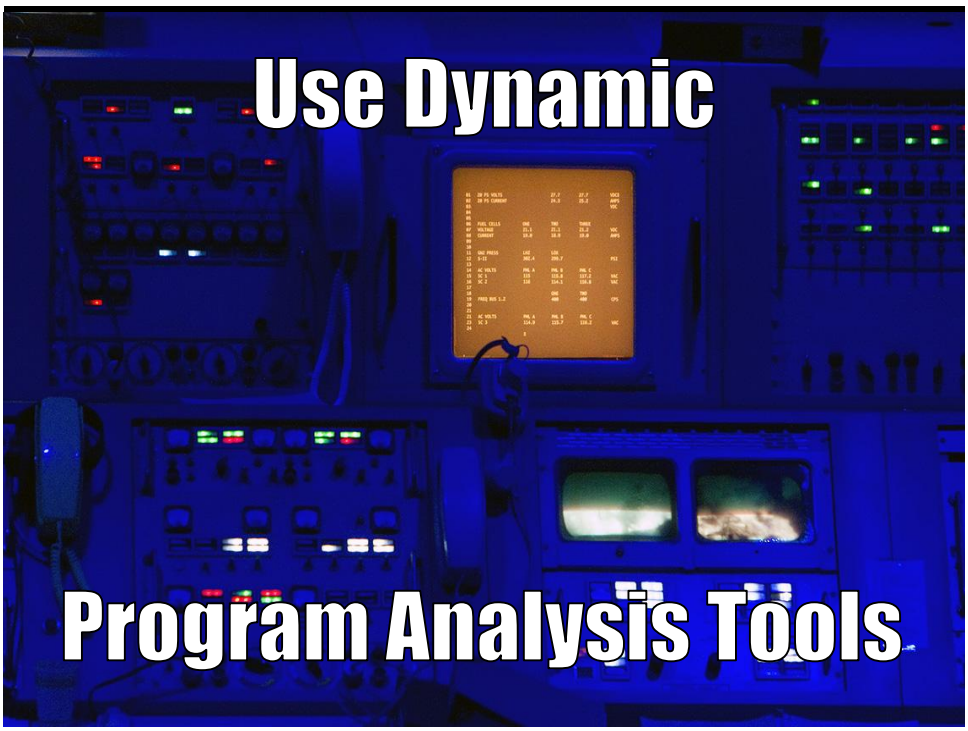

Runtime Techniques
GOT 'EM!

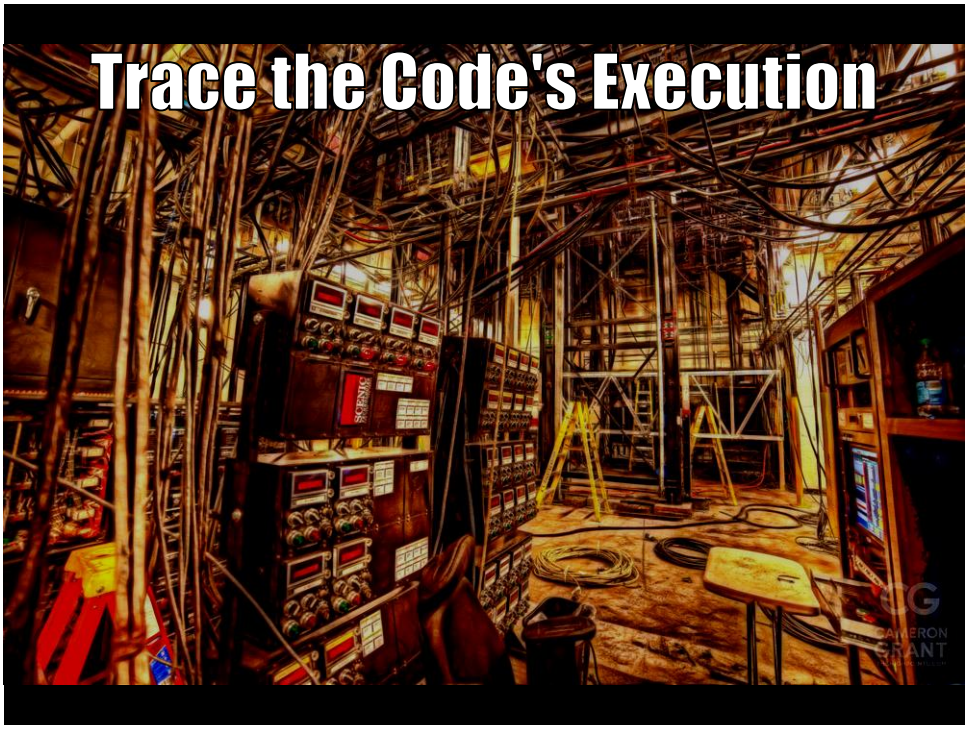

Find the Fault
by Constructing a Test Case


Fail
FAST


Examine
Application Log Files
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Hardware Events
Internet Explorer
Key Management Service
Media Center
Microsoft
Windows
API-Tracing
AppID
Application Server-Applications
Application-Experience
AppLocker
Audio
Authentication
Authentication User Interface
Backup
Biometrics
Bits-Client
Bluetooth-MTPEnum
BranchCache
BranchCacheSMB
CAPI2
CertificateServicesClient-Credentia
CertPolEng
CodeIntegrity
Compat-Appraiser
DateTimeCo
DeviceSync
Dhcp-Client
Dhcp-Nap-Enforcement-Client
System
Level
Event ID
Task C
Information 04/06/2016 15:56:16 Kernel-General 1 None
Information 04/06/2016 15:43:30 Kernel-General 1 None
Information 04/06/2016 15:43:27 Kernel-Power 42 (64)
Information 04/06/2016 15:43:27 BROWSER 8033 None
Error 04/06/2016 15:43:24 Smart Card Service 610 None
Error 04/06/2016 15:43:24 Smart Card Service 610 None
Information 04/06/2016 15:43:24 Service Control Mana... 7036 None
Error 04/06/2016 15:43:24 Smart Card Service 610 None
Error 04/06/2016 15:43:24 Smart Card Service 610 None
Error 04/06/2016 15:43:18 AX88772 48 None
Information 04/06/2016 15:33:43 Service Control Mana... 7036 None
Information 04/06/2016 15:22:21 Service Control Mana... 7036 None
Information 04/06/2016 15:18:46 Service Control Mana... 7036 None
Information 04/06/2016 15:17:16 Service Control Mana... 7036 None
Information 04/06/2016 15:17:13 Service Control Mana... 7036 None
Information 04/06/2016 15:16:21 Service Control Mana... 7036 None
Information 04/06/2016 15:03:13 Service Control Mana... 7036 None
Information 04/06/2016 14:59:51 Service Control Mana... 7036 None
Information 04/06/2016 14:55:05 Service Control Mana... 7036 None
General Details
Smart Card Reader 'Gemalto USB Smart Card Reader 0' rejected IOCTL TRANSMIT: The request could not be performed because of an I/O device error. If this error persists, your smart card or reader may not be functioning correctly.
Log Name: System
Logged: 04/06/2016 15:43:24
More Information:
Actions
System
Open Saved L...
Create Custo...
Import Custo...
Clear Log...
Filter Current ...
Properties
Find...
Save All Even...
Attach a Task...
View
Refresh
Help
Event 610, Smar...
Event Propert...
Attach Task T...
Copy
Save Selected...
Refresh
Help


Profile the Operation
of Systems and Processes
Oracle Java Mission Control
File Edit Window
JVM Browser
[1.8.0_73] C:\Pro
MBean Server
Flight Recorder
[1.8.0_73] The JVM Running Mission
MBean Server
Flight Recorder
General
Memory
Code
Threads
I/O
System
Events
Events Operative Set
Interval: 59 s 966 ms (all)
Synchronize Selection
12/02/16 18:40:41
12/02/16 18:41:41
Hot Packages
The packages where the application spent most time executing.
Package
Sample Count
Percentage
java.awt 7 17.95%
javax.swing 4 10.26%
java.util 3 7.69%
java.io 2 5.13%
sun.java2d 2 5.13%
javax.swing.text 2 5.13%
org.freeplane.view.swing.map 2 5.13%
javax.swing.plaf.basic 2 5.13%
com.oracle.jrockit.jfr 1 2.56%
javax.swing.text.html 1 2.56%
java.util.regex 1 2.56%
Hot Classes
Filter Column Class
Class
Sample Count
Percentage
java.awt.Container 4 10.26%
javax.swing.SwingUtilities 2 5.13%
javax.swing.plaf.basic.BasicLabelUI 2 5.13%
com.oracle.jrockit.jfr.InstantEvent 1 2.56%
java.io.ObjectInputStream$BlockDataInputStream 1 2.56%
sun.java2d.SunGraphics2D 1 2.56%
javax.swing.RepaintManager 1 2.56%
javax.swing.TimerQueue$DelayedTimer 1 2.56%
2.56%
2.56%
2.56%
Overview
Hot Methods
Call Tree
Exceptions
Compilations
Class Loading


Use Dynamic
Program Analysis Tools


Trace the Code's Execution


Got them all?
GOT 'EM!

Thank you!

dds@aueb.gr
www.spinellis.gr
@CoolSWEng
github.com/dspinellis

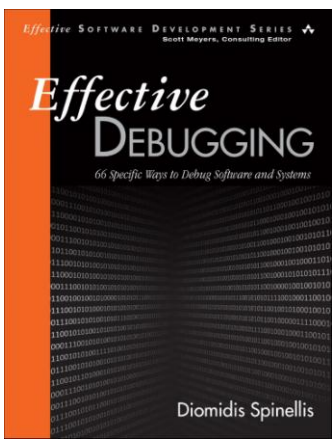


Image credits

- Server rack: Jfreyre; CC BY-SA 3.0
- Engage: InnovateOSU; CC BY 2.0
- Winpdb: Nir Aides; CC BY-SA 3.0
- Serial killer: Thomas Hawk; CC BY-NC 2.0
- O RLY? covers: @ThePracticalDev
- Drill: Palmer, Alfred T.; PD
- Twin statues: The Children's Museum of Indianapolis; CC BY-SA 3.0
- Sleeping: Andrew Roberts; CC BY 2.0
- Wootton Bridge after the crash: PD
- The Rubber Duck: Francisco Martins; CC BY-NC 2.0
- Fuse: Razor512; CC BY 2.0
- K&R on a PDP11: Peter Hamer; CC BY-SA 2.0
- Core memory: Bubba73 (Jud McCranie); CC BY-SA 4.0
- Three Monitors: Mike Shoup; CC BY-NC 2.0
- Leviathan Dismantled: Cameron Grant; CC BY-NC-SA 2.0
- Marzipan Dolls: Alan; CC BY 2.0
- "Working": chris riebschlager; CC BY-NC 2.0
- Router debugging: Speshul Ted; CC BY-NC-SA 2.0
- Tuning: Kalle Hyttinen; CC BY-NC 2.0
- Program Listing: Scott Schiller; CC BY-NC 2.0
- Reverse: Catalina Olavarria; CC BY-NC-SA 2.0
- New Yorkers like to check out the scene: Ed Yourdon! CC BY-NC-SA 2.0
- Electronic cityscape: kerolic; CC BY-NC-SA 2.0
- Deadlock: Ercument Sener; CC BY-NC-SA 2.0
- Editing with reel to reel tape: Jonathan Marks; CC BY-NC-SA 2.0
- Tricking: Zirklerankes galerija; CC BY-NC-SA 2.0
- Control Room Panel: Jonathan Haeber; CC BY-NC 2.0
- Illness: Liz Wade; CC BY-NC 2.0
- Kinemetrics seismograph: Yamaguchi; CC BY-SA 3.0
- Balance: M Cheung; CC BY-NC 2.0
- Meat grinder: ppank_l; CC BY-NC-SA 2.0
- Iceberg: Uwe Kils (iceberg) and Wiska Bodo (sky); CC BY-SA 3.0
- Decaying threshing machine: Neil Howard ; CC BY-NC 2.0
- Boeing: Jennifer Reitz/Boeing
- Nairobi Forest Preserve: Aaron Knox; CC BY-NC-SA 2.0
- Gource visualization: Landon Wilkins
- cat & dog: b1ue5ky; CC BY-NC-SA 2.0
- Business Round Table: Juerg Stuker; CC BY-NC 2.0
- Belay setup: Oliver Frank; CC BY-NC-SA 2.0
- Mr . Happy Hat: Nick Kenrick (texture by Joes sistah); CC BY-NC-SA 2.0
- Small-Big: J-Ron North ; CC BY-NC_SA 2.0

- License links: CC BY 2.0 , CC BY-SA 2.0 , CC BY-SA 3.0 , CC BY-SA 4.0, CC BY-NC 2.0 , CC BY-NC-SA 2.0