

Execution Synthesis

Brendan Cully, Geoffrey Lefebvre,
Dutch T. Meyer, Norman C. Hutchinson,
Andrew Warfield
The University of British Columbia



Get Directions | [My Maps](#) ⏪

✕

A

B

[Add Destination](#) - [Show options](#)

▾

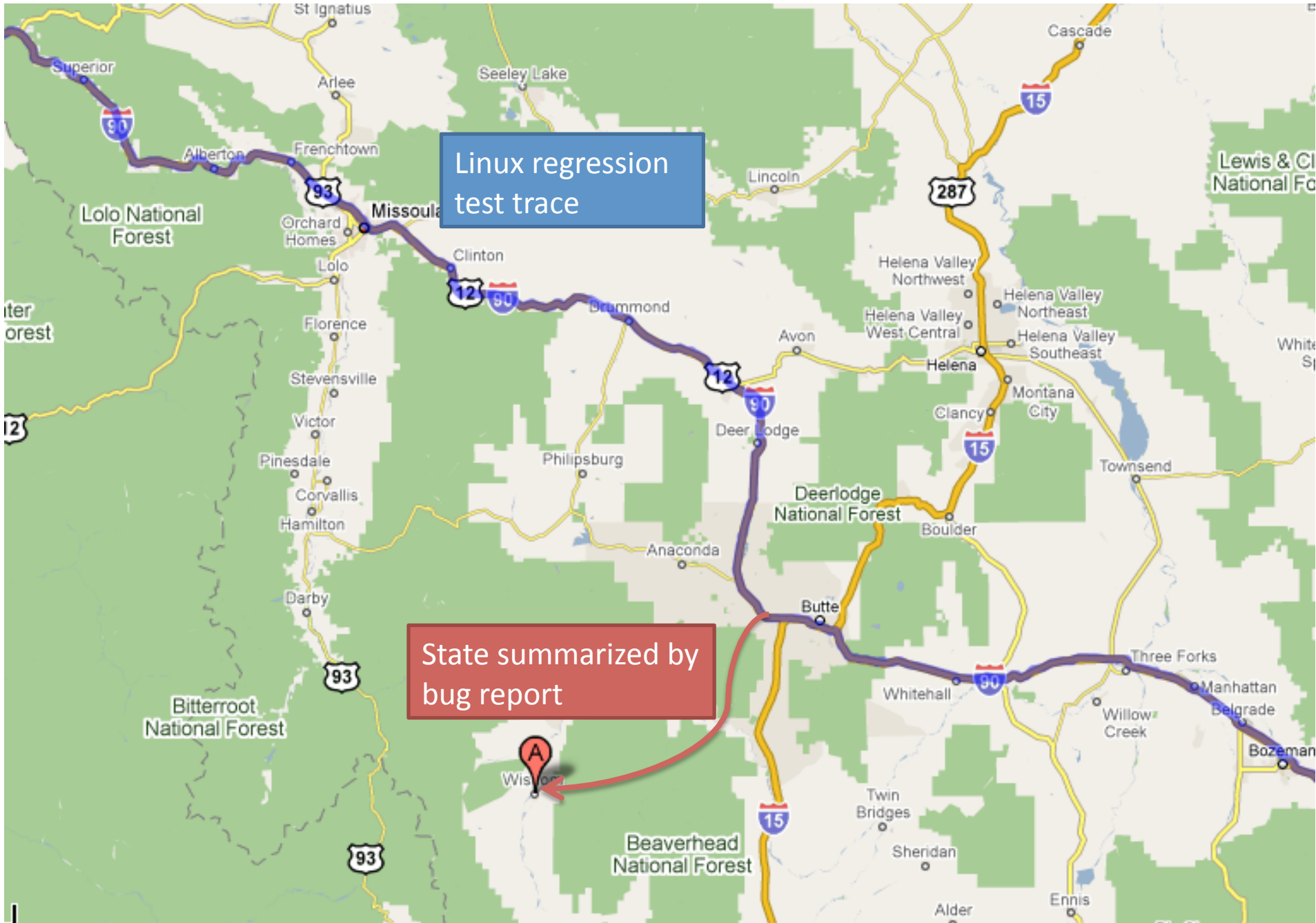
➤

We could not calculate directions between **linux 2.6.24.8** and **BUG: unable to handle kernel paging request at c0413130.c**



==

```
BUG: unable to handle kernel paging request at vi
printing eip: c031d441 *pde = 004001e3
Oops: 0003 [#1] SMP
Pid: 0, comm: swapper Not tainted (2.6.24-24-gene
EIP: 0060:[<c031d441>] EFLAGS: 00010082 CPU: 0
EIP is at _spin_lock+0x1/0x10
EAX: c0413130 EBX: c0413100 ECX: 00d8b000 EDX: c0
ESI: 00000005 EDI: 00000000 EBP: c0413130 ESP: c0
DS: 007b ES: 007b FS: 00d8 GS: 0000 SS: 0068
Process swapper (pid: 0, ti=c041e000 task=c03eb3a
Stack: c016a0b7 00000280 c0413100 00000000 000000
c0118895 00000000 c0478004 c047e300 000068
c041e000 c0478004 c047e300 000068a0 000000
Call Trace:
[<c016a0b7>] handle_level_irq+0x27/0xf0
[<c0106f0b>] do_IRQ+0x3b/0x70
[<c0118895>] smp_apic_timer_interrupt+0x55/0x80
[<c0105403>] common_interrupt+0x23/0x30
[<c0102f40>] default_idle+0x0/0x60
[<c011ebf2>] native_safe_halt+0x2/0x10
```



Linux regression test trace

State summarized by bug report

A

Open questions

- Distance function
- Choosing inputs to inject
- What data to include in a bug report

Execution Synthesis

- ① Record normal execution (e.g. regression test suite)
- ② Identify “nearby” starting points
- ③ Drive execution into the weeds

Lather, rinse, repeat

I'm Feeling Lucky