



# Debugging.TV

Frame 0x0F

Presenter: Dmitry Vostokov

MEMORY DUMP ANALYSIS SERVICES

[DumpAnalysis.com](http://DumpAnalysis.com)

Including Crash and Hang Analysis Audit, Training and Seminars

Sponsors

**OPENTASK**

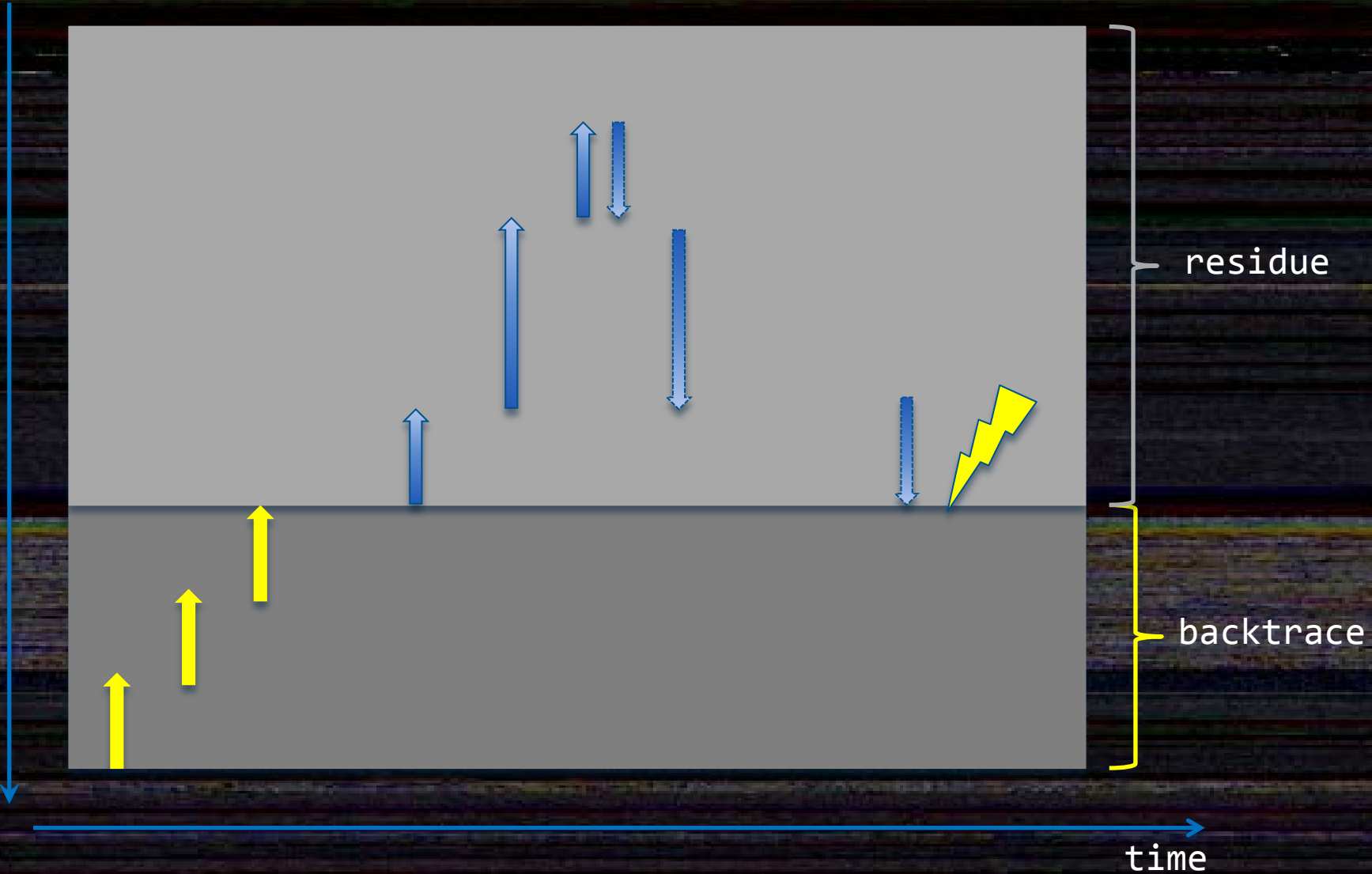
Iterative and Incremental Publishing

# Topics

- Raw stack
- Execution Residue pattern
- Effect Component pattern

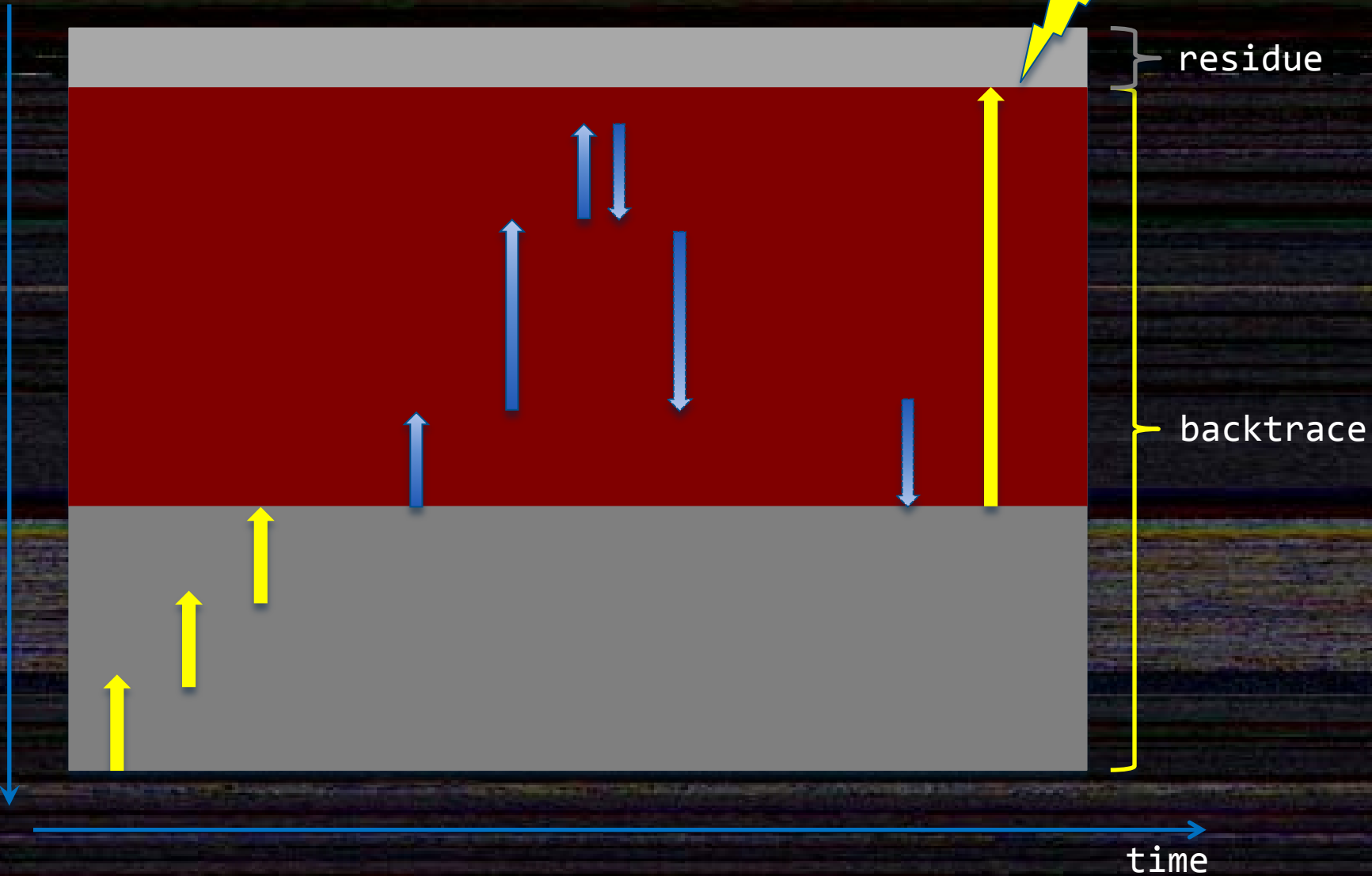
# Raw Stack

address



# Absent Residue

address



# GDB Output (no residue)

(gdb) **bt**

```
#0 0x00007fff8616e82a in __kill ()
#1 0x00007fff8fab9a9c in abort ()
#2 0x000000010e3c7c39 in bar_5 ()
#3 0x000000010e3c7c49 in bar_4 ()
#4 0x000000010e3c7c59 in bar_3 ()
#5 0x000000010e3c7c69 in bar_2 ()
#6 0x000000010e3c7c79 in bar_1 ()
#7 0x000000010e3c7c89 in bar ()
#8 0x000000010e3c7cb0 in main (argc=1, argv=0x7fff6dfc6b00)
```

(gdb) **x \$rsp**

```
0x7fff6dfc6a38:      0x8fab9a9c
```

(gdb) **x/1000a 0x7fff6dfc6000**

[...]

```
0x7fff6dfc6a30:      0x7fff6dfc6a60      0x7fff8fab9a9c <abort+177>
0x7fff6dfc6a40:      0x0      0x0
0x7fff6dfc6a50:      0x7fffffffdf      0x0
0x7fff6dfc6a60:      0x7fff6dfc6a70      0x10e3c7c39 <bar_5+9>
0x7fff6dfc6a70:      0x7fff6dfc6a80      0x10e3c7c49 <bar_4+9>
0x7fff6dfc6a80:      0x7fff6dfc6a90      0x10e3c7c59 <bar_3+9>
0x7fff6dfc6a90:      0x7fff6dfc6aa0      0x10e3c7c69 <bar_2+9>
0x7fff6dfc6aa0:      0x7fff6dfc6ab0      0x10e3c7c79 <bar_1+9>
0x7fff6dfc6ab0:      0x7fff6dfc6ac0      0x10e3c7c89 <bar+9>
0x7fff6dfc6ac0:      0x7fff6dfc6ae0      0x10e3c7cb0 <main+32>
0x7fff6dfc6ad0:      0x7fff6dfc6b00      0x1
0x7fff6dfc6ae0:      0x7fff6dfc6af0      0x10e3c7b84 <start+52>
```

[...]

# GDB Output (residue)

(gdb) x \$rsp

0x7fff6b714a38: 0x8fab9a9c

(gdb) x/1000a 0x7fff6b714000

[...]

0x7fff6b714610:	0x100000000	0xbb15000
0x7fff6b714620:	0x7fff6b714630	0x10bb15b59 <foo_8+9>
0x7fff6b714630:	0x7fff6b714640	0x10bb15b69 <foo_7+9>
0x7fff6b714640:	0x7fff6b714650	0x10bb15b79 <foo_6+9>
0x7fff6b714650:	0x7fff6b714660	0x10bb15b89 <foo_5+9>
0x7fff6b714660:	0x7fff6b714670	0x10bb15b99 <foo_4+9>
0x7fff6b714670:	0x7fff6b714680	0x10bb15ba9 <foo_3+9>
0x7fff6b714680:	0x7fff6b714690	0x10bb15bb9 <foo_2+9>
0x7fff6b714690:	0x7fff6b7146a0	0x10bb15bc9 <foo_1+9>
0x7fff6b7146a0:	0x7fff6b714ac0	0x10bb15bee <foo+30>
0x7fff6b7146b0:	0x0	0x0
[...]		
0x7fff6b714a50:	0xfffffffffd	0x0
0x7fff6b714a60:	0x7fff6b714a70	0x10bb15c29 <bar_5+9>
0x7fff6b714a70:	0x7fff6b714a80	0x10bb15c39 <bar_4+9>
0x7fff6b714a80:	0x7fff6b714a90	0x10bb15c49 <bar_3+9>
0x7fff6b714a90:	0x7fff6b714aa0	0x10bb15c59 <bar_2+9>
0x7fff6b714aa0:	0x7fff6b714ab0	0x10bb15c69 <bar_1+9>
0x7fff6b714ab0:	0x7fff6b714ac0	0x10bb15c79 <bar+9>
0x7fff6b714ac0:	0x7fff6b714ae0	0x10bb15ca0 <main+32>
0x7fff6b714ad0:	0x7fff6b714b00	0x1
0x7fff6b714ae0:	0x7fff6b714af0	0x10bb15b34 <start+52>
0x7fff6b714af0:	0x0	0x1



# !Ad Hardcore Technical Support Training

June 22, 2012	<a href="#"><u>Introduction to Pattern-Driven Software Diagnostics</u></a> (Free Webinar)
June 29, 2012	<a href="#"><u>Victimware: The Missing Part of the Equation</u></a> (Free Webinar)
July 18-23, 2012	<a href="#"><u>Accelerated Windows Memory Dump Analysis</u></a>
July 27-30, 2012	<a href="#"><u>Accelerated Mac OS X Core Dump Analysis</u></a>
Sept 14-17, 2012	<a href="#"><u>Advanced Windows Memory Dump Analysis</u></a>
October 12-15, 2012	<a href="#"><u>Accelerated Windows Software Trace Analysis</u></a>
October 17-22, 2012	<a href="#"><u>Accelerated Windows Malware Analysis</u></a>

# Debugging.TV

Debugging TV soon joins DEMO (Debugging Experts Magazine Online)

[www.debuggingexperts.com](http://www.debuggingexperts.com)