Debugging.TV

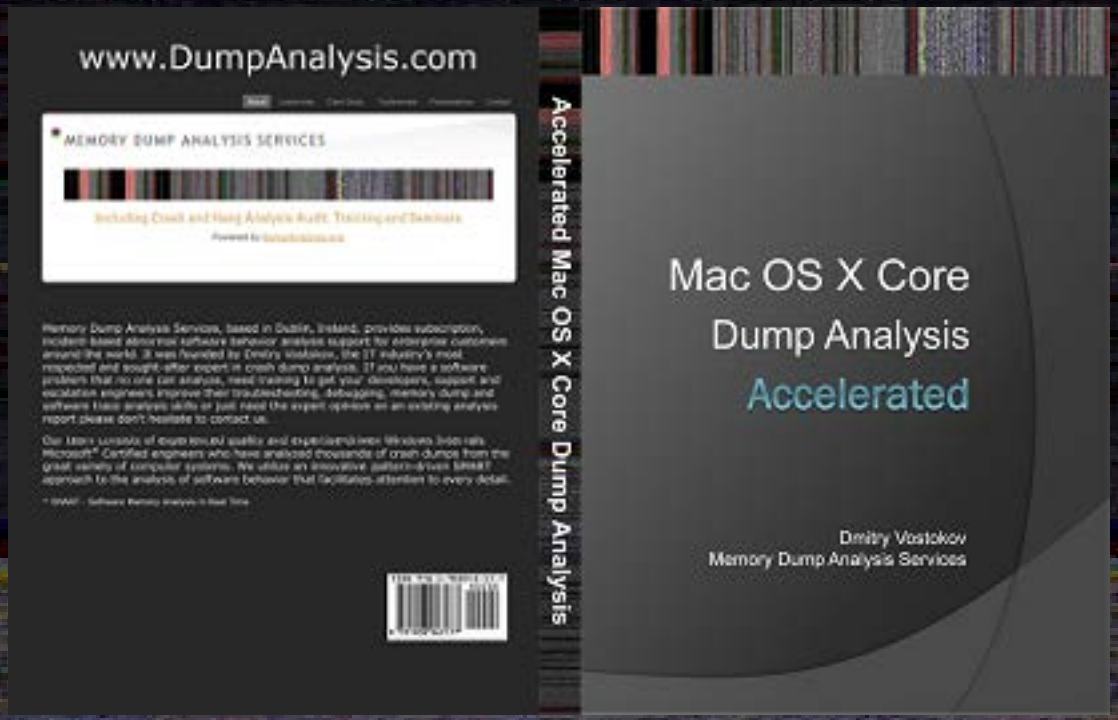
Frame 0x12

Presenter: Dmitry Vostokov

Topics

- Software Diagnostics Pattern Language for Mac OS
- Core Dump Analysis Pattern Interaction Example
- Partial Stack Trace Reconstruction

Patterns for Mac OS X



ISBN: 978-1908043405

Truncated Stack Trace

```
DumpAnalysis$ ls -l /cores
total 2357440
-r--------  1 root          admin  301752320  1 Aug 02:35 core.103
-r--------  1 root          admin  301752320  1 Aug 02:45 core.107
-r--------  1 root          admin  301752320  1 Aug 02:23 core.148
-r--------  1 DumpAnalysis  admin          0  1 Aug 02:46 core.413
-r--------  1 root          admin  301752320  1 Aug 02:30 core.78

DumpAnalysis$ sudo gdb -c /cores/core.103

(gdb) bt
#0  0x00045d6c in l2_packet_receive ()
#1  0x8fea1c9c in ?? ()
Previous frame inner to this frame (gdb could not unwind past this frame)
```

Execution Residue

```
(gdb) x/1000a $esp-1000
[…]
0xbffffa48: 0x0         0x9a5664c4 <vsnprintf+12>          0x91796 <pcap_read_bpf+17>          0x99
0xbffffa58: 0xbffffa78  0x9a566502 <vsnprintf+74>          0xbffffaf8  0x100
[…]
0xbffffa68: 0xacda7524 <__global_locale>        0x9a81c    0x91796 <pcap_read_bpf+17>          0xbffffc28
0xbffffa78: 0xbffffa98  0x920b1 <pcap_oneshot+35>          0xbffffc58  0xbffffae8
[…]
0xbffffa88: 0x110       0xbffffab4  0xbffffab4  0x300000
0xbffffa98: 0xbffffc08  0x91b1c <pcap_read_bpf+919>        0xbffffc28  0xbffffae8
[…]
0xbffffbf8: 0x0         0x45d2d <l2_packet_receive>        0x8a9800    0x8ba0 <eloop_run+12>
0xbffffc08: 0xbffffc38  0x91feb <pcap_next+58>  0x8a9800   0x1
[…]
0xbffffc28: 0xbffffc58  0xbffffc24  0x8a9800    0x0
0xbffffc38: 0xbffffc88  0x45d52 <l2_packet_receive+37>     0x8a9800    0xbffffc58
[…]
0xbffffc78: 0x37323335  0x30373833  0x76732037  0x45422063
0xbffffc88: 0x8fe9e100  0x8fea1c9c  0x0         0x1a3500
[…]
0xbffffd58: 0x0         0x0         0xff0000    0xffffff
0xbffffd68: 0xbffffdd8  0x43c04 <main+1143> 0x2084a0       0x208200
[…]
0xbffffdc8: 0x0         0x2084a0    0xbffffe28  0x0
0xbffffdd8: 0xbffffdf0  0x2356 <start+54>       0x5        0xbffffdf8
```

Regular Buffer

```
0xbffffc38:  0xbffffc88  0x45d52 <l2_packet_receive+37>          0x8a9800     0xbffffc58
0xbffffc48:  0xbffffc58  0x9a4e5ca4 <__commpage_gettimeofday+20> 0x0          0xbffffca4
0xbffffc58:  0x50185dbe  0x7a161      0x99          0x99
0xbffffc68:  0x20646970  0x72f240e8   0x300012      0x300012
0xbffffc78:  0x37323335  0x30373833   0x76732037    0x45422063
0xbffffc88:  0x8fe9e100  0x8fea1c9c   0x0           0x1a3500
0xbffffc98:  0xbffffba8  0x91fb1 <pcap_next>        0x5e35c <dyld_stub_pcap_lookupnet+2>   0x364
0xbffffca8:  0x4d00030c  0x7863c      0x33c4de9     0x41d7e900
0xbffffcb8:  0xacdac044 <__is_threaded> 0x1464      0x8fea1c9c   0x5e35f <dyld_stub_pcap_next>
0xbffffcc8:  0xbffffba8  0x8fe824c8   0x8fea1c9c    0x5e35f <dyld_stub_pcap_next>
0xbffffcd8:  0x1464      0x786bc      0x91fb1 <pcap_next>        0x8fea27cc
0xbffffce8:  0x8fe9e140  0x1000002    0x8fe8234e    0x11
0xbffffcf8:  0x4         0x13e8       0x71354       0x786bc
0xbffffd08:  0x8fea27cc  0x5e364 <dyld_stub_pcap_open_live>      0x8fe6eefb   0x8ba0 <eloop_run+12>
0xbffffd18:  0xbffffbc8  0x8fe6ef6f   0x8fea1c9c    0x5e364 <dyld_stub_pcap_open_live>
0xbffffd28:  0x8fe9e140  0x9a513557 <malloc_zone_malloc+75>      0x45d2d <l2_packet_receive>            0x8a9800
0xbffffd38:  0xbffffc38  0x8fe7fdbe   0x0           0x5e364 <dyld_stub_pcap_open_live>
0xbffffd48:  0xbffffc08  0x1a0000     0x0           0x0
0xbffffd58:  0x0         0x0          0xff0000      0xffffff
0xbffffd68:  0xbffffdd8  0x43c04 <main+1143>        0x2084a0     0x208200
0xbffffd78:  0x59ec0 <base64_table+12068>           0xbffffdf8   0xbffffe10   0xbffffe28
```

```
(gdb) x/s 0xbffffc78
0xbffffc78:          "532738707 svc BE"
```

!Ad Hardcore Technical Support Training

Sept 3, 2012	Systemic Software Diagnostics (FREE Webinar)
October 12-15, 2012	Accelerated Windows Software Trace Analysis
November 16-26, 2012	Accelerated Windows Memory Dump Analysis
November 2-5, 2012	Accelerated Mac OS X Core Dump Analysis
December 7-10, 2012	Accelerated Windows Malware Analysis

Debugging³

Forthcoming in December, 2012

Debugging.TV