



Debugging.TV

Frame 0x0E

Presenter: Dmitry Vostokov

MEMORY DUMP ANALYSIS SERVICES

DumpAnalysis.com

Including Crash and Hang Analysis Audit, Training and Seminars

Sponsors

OPENTASK

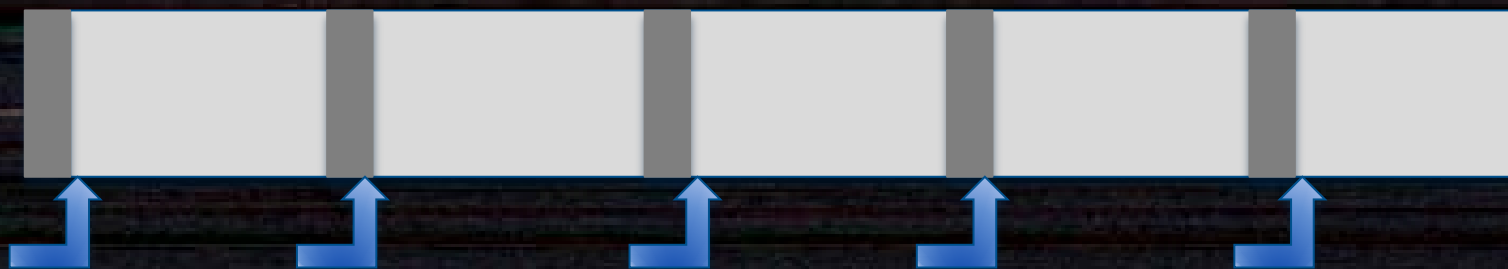
Iterative and Incremental Publishing

Topics

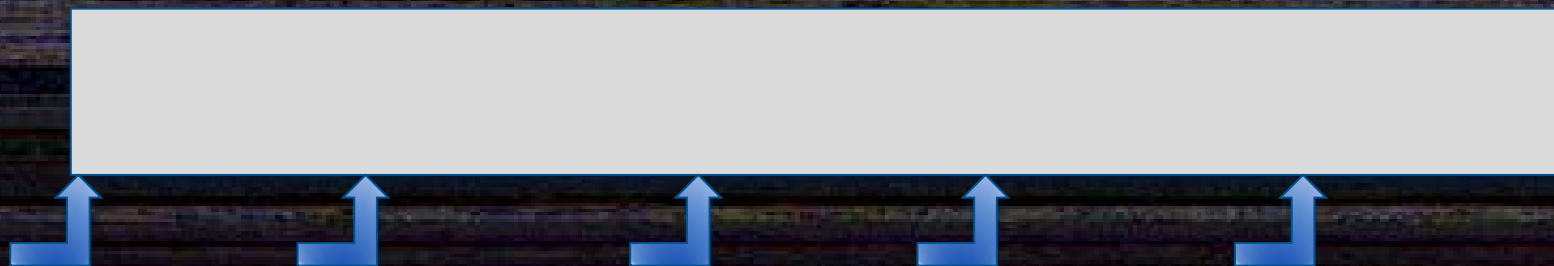
- Heap on Mac OS X vs. Windows
- Heap Corruption pattern
- Double Free pattern

Heap (allocated)

- Windows

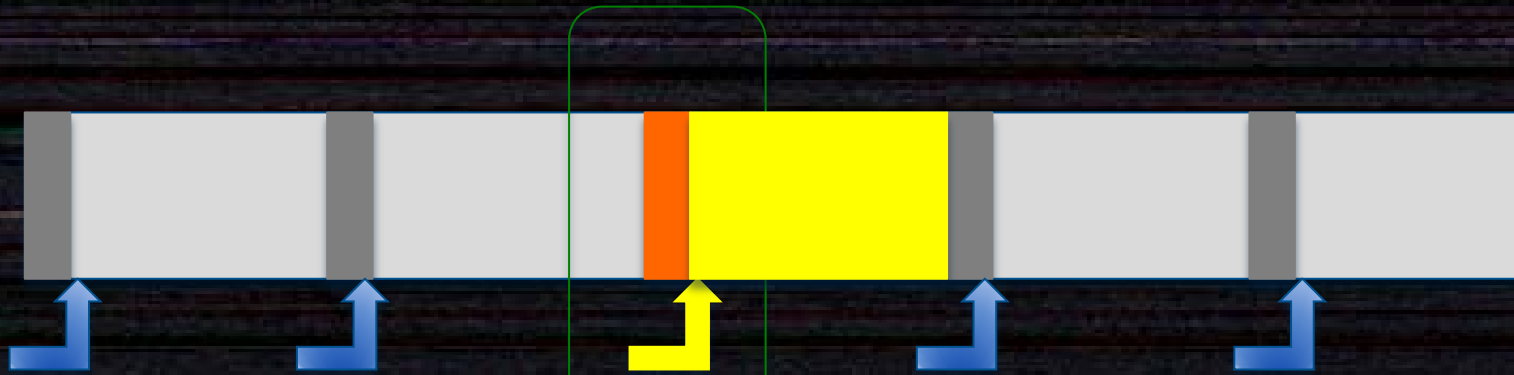


- Mac OS X

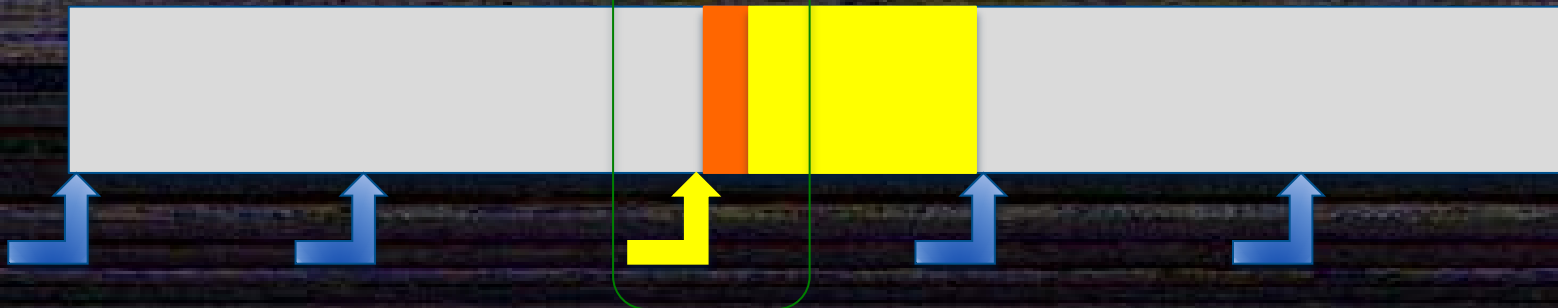


Heap (free)

- Windows



- Mac OS X



Heap Corruption

```
{
    free(p6);
    free(p4);
    free(p2);

    strcpy(p2, "Hello Crash!");
    strcpy(p4, "Hello Crash!");
    strcpy(p6, "Hello Crash!");

    p2 = (char *) malloc (512);
    printf("p2 = %p\n", p2);

    p4 = (char *) malloc (1024);
    printf("p4 = %p\n", p4);

    p6 = (char *) malloc (512);
    printf("p6 = %p\n", p6);

    free (p7);
    free (p6);
    free (p5);
}
```

```
DumpAnalysis$ ../HeapCorruption2/Build/Products/Debug/HeapCorruption2
```

```
...
```

```
p2 = 0x107000890
```

```
p4 = 0x7fd613801400
```

```
p6 = 0x107000a90
```

```
HeapCorruption2(477) malloc: *** error for object 0x7fd613802408: incorrect checksum for freed object - object was probably modified after being freed.
```

```
...
```

GDB Output

(gdb) **bt**

```
#0 0x00007fff8479582a in __kill ()
#1 0x00007fff8e0e0a9c in abort ()
#2 0x00007fff8e1024ac in szone_error ()
#3 0x00007fff8e1024e8 in free_list_checksum_botch ()
#4 0x00007fff8e102a7b in small_free_list_remove_ptr ()
#5 0x00007fff8e106bf7 in szone_free_definite_size ()
#6 0x00007fff8e13f789 in free ()
#7 0x0000000106f21e23 in main (argc=1, argv=0x7fff66b20b08)
```

(gdb) **frame 7**

```
#7 0x0000000106f21e23 in main (argc=1, argv=0x7fff66b20b08)
    at ../HeapCorruption2/main.c:56
56      free (p5);
```

(gdb) **x/2i** 0x0000000106f21e23

```
0x106f21e23 <main+771>:      mov     -0x30(%rbp),%rdi
0x106f21e27 <main+775>:      callq  0x106f21e9a <dyld_stub_free>
```

(gdb) **x/s** 0x7fd613802408

```
0x7fd613802408:      "ash!"
```

!Ad Hardcore Technical Support Training

June 22, 2012	<u>Introduction to Pattern-Driven Software Diagnostics</u> (Free Webinar)
June 29, 2012	<u>Victimware: The Missing Part of the Equation</u> (Free Webinar)
July 11-16, 2012	<u>Accelerated Windows Memory Dump Analysis</u>
July 20-23, 2012	<u>Advanced Windows Memory Dump Analysis</u>
July 27-30, 2012	<u>Accelerated Mac OS X Core Dump Analysis</u>
October 12-15, 2012	<u>Accelerated Windows Software Trace Analysis</u>
October 17-22, 2012	<u>Accelerated Windows Malware Analysis</u>

Debugging.TV