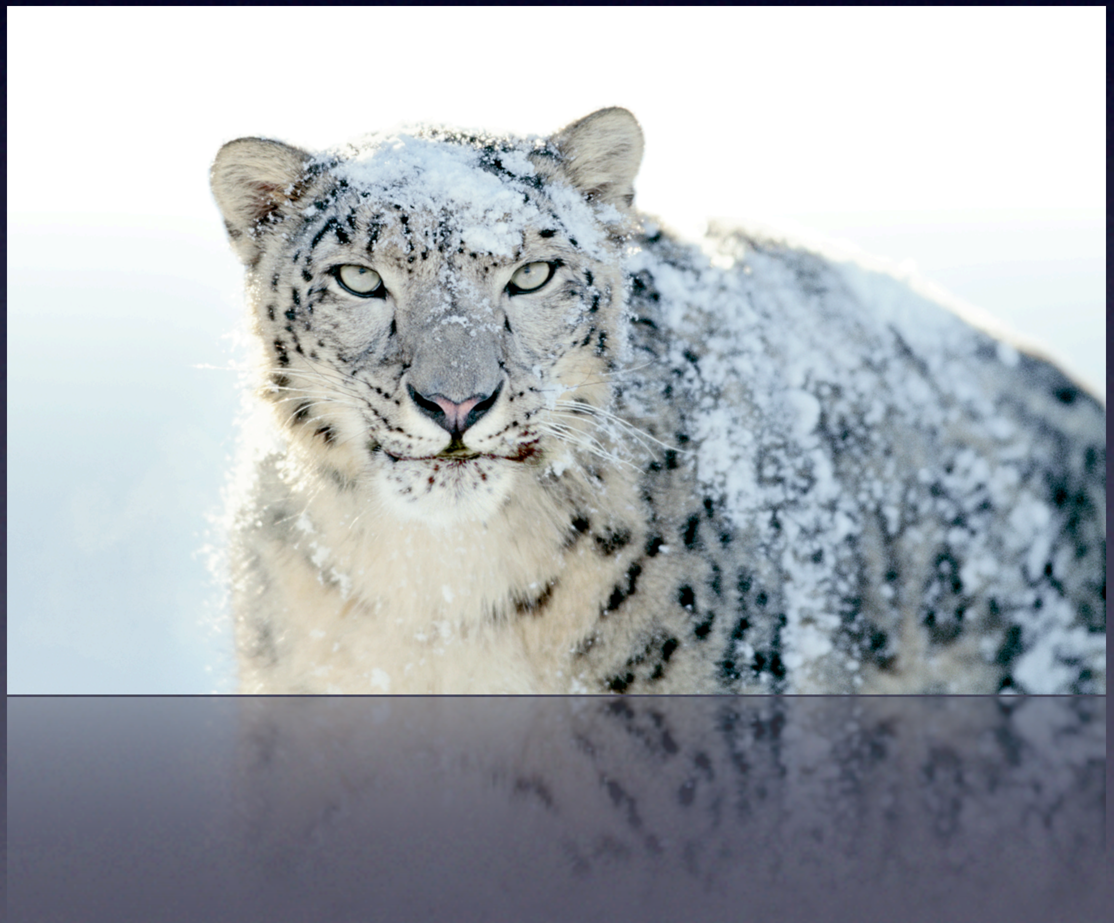
FruityFuzz

A Simple Mutation-Based File Fuzzer for Mac

Jordan Schau
5/2/11

Requirements

- Easy to use
- Versatile
- Fast
- Work with current OS X 10.6.X



Current State

- PeachFuzz - http://peachfuzzer.com/
- Sulley - http://code.google.com/p/sulley/
- Generally Poor Documentation for Mac

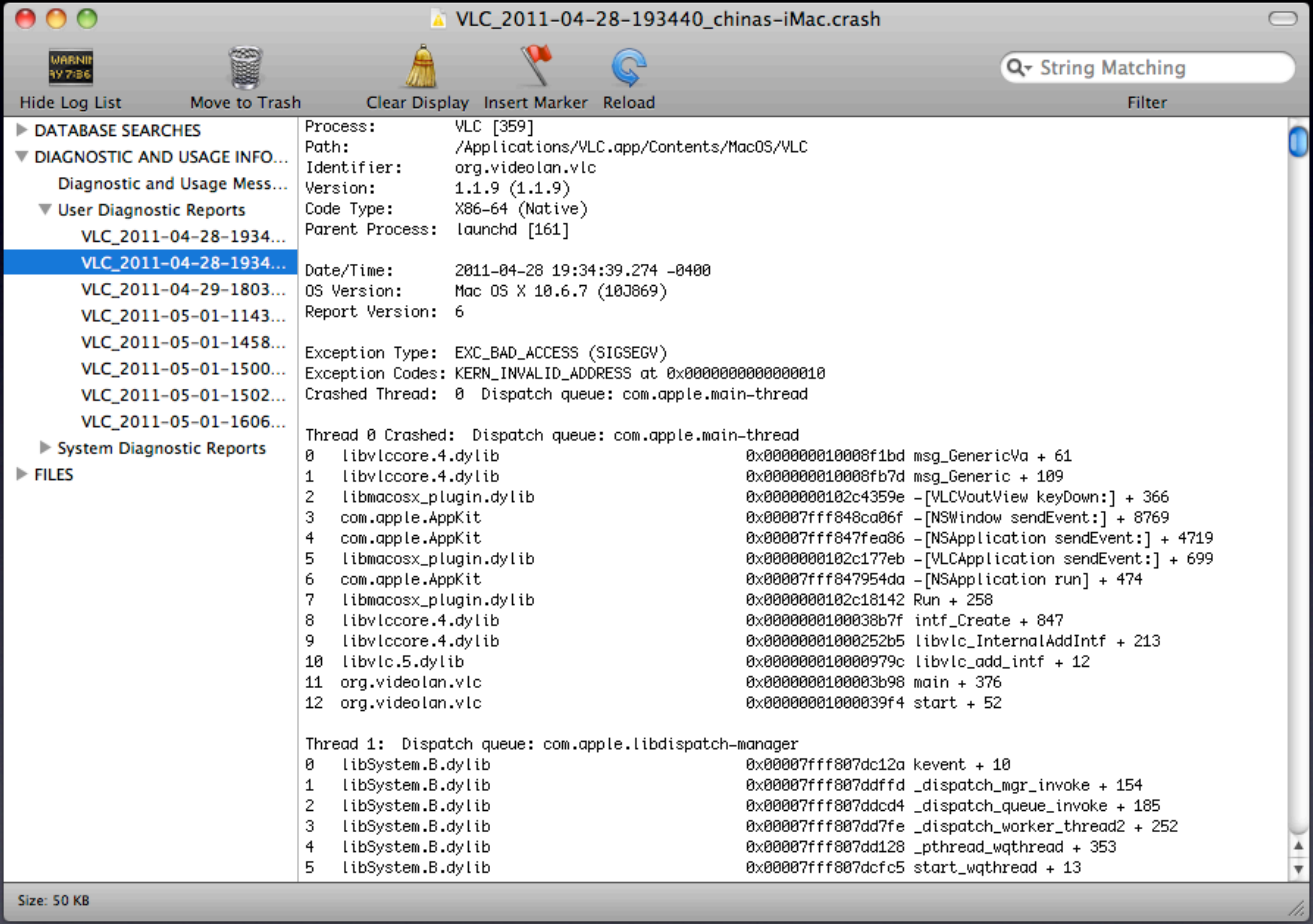
A bit about Mac OS X Snow Leopard

- Most processes are 64 bit
  - Different Register System
    - Moved from 8 registers to 16
- ASLR not fully implemented
  - Only used for certain library offsets

Tools Used

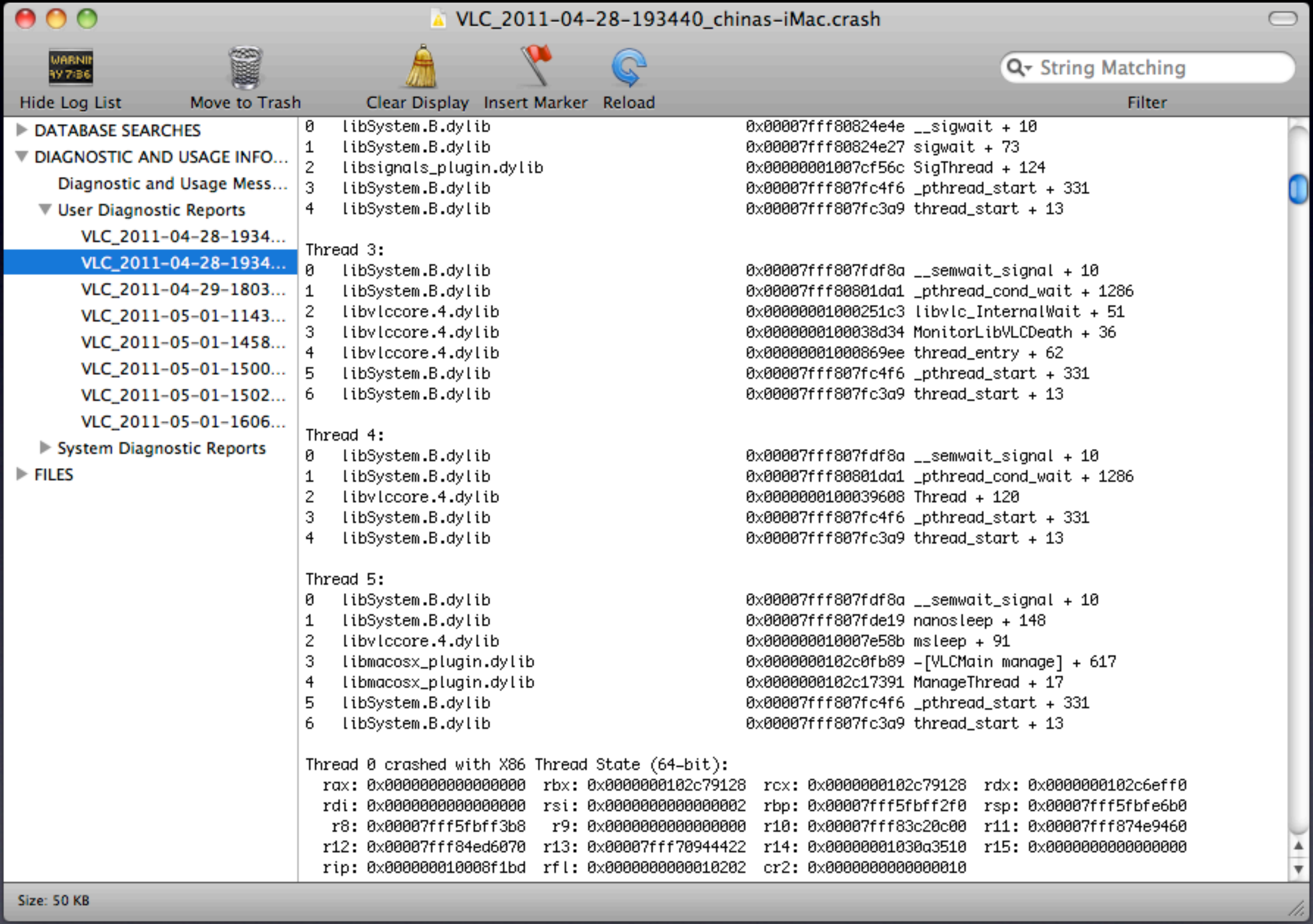
- Python 2.7
  - Good: High Level file I/O
  - Bad: Multithreading and forking child processes
- CrashReporter
  - Good reporting of crash
  - Crash Reports are deleted after 20 are found

Crash Reporter



```
Process:         VLC [359]
Path:            /Applications/VLC.app/Contents/MacOS/VLC
Identifier:      org.videolan.vlc
Version:         1.1.9 (1.1.9)
Code Type:       X86-64 (Native)
Parent Process:  launchd [161]

Date/Time:       2011-04-28 19:34:39.274 -0400
OS Version:      Mac OS X 10.6.7 (10J869)
Report Version:  6

Exception Type:  EXC_BAD_ACCESS (SIGSEGV)
Exception Codes: KERN_INVALID_ADDRESS at 0x0000000000000010
Crashed Thread:  0  Dispatch queue: com.apple.main-thread

Thread 0 Crashed:  Dispatch queue: com.apple.main-thread
0   libvlccore.4.dylib              0x000000010008f1bd msg_GenericVa + 61
1   libvlccore.4.dylib              0x000000010008fb7d msg_Generic + 109
2   libmacosx_plugin.dylib          0x0000000102c4359e -[VLCVoutView keyDown:] + 366
3   com.apple.AppKit                0x00007fff848ca06f -[NSWindow sendEvent:] + 8769
4   com.apple.AppKit                0x00007fff847fea86 -[NSApplication sendEvent:] + 4719
5   libmacosx_plugin.dylib          0x0000000102c177eb -[VLCApplication sendEvent:] + 699
6   com.apple.AppKit                0x00007fff847954da -[NSApplication run] + 474
7   libmacosx_plugin.dylib          0x0000000102c18142 Run + 258
8   libvlccore.4.dylib              0x000000010038b7f intf_Create + 847
9   libvlccore.4.dylib              0x00000001000252b5 libvlc_InternalAddIntf + 213
10  libvlc.5.dylib                  0x000000010000979c libvlc_add_intf + 12
11  org.videolan.vlc                0x0000000100003b98 main + 376
12  org.videolan.vlc                0x00000001000039f4 start + 52

Thread 1:  Dispatch queue: com.apple.libdispatch-manager
0   libSystem.B.dylib               0x00007fff807dc12a kevent + 10
1   libSystem.B.dylib               0x00007fff807ddffd _dispatch_mgr_invoke + 154
2   libSystem.B.dylib               0x00007fff807ddcd4 _dispatch_queue_invoke + 185
3   libSystem.B.dylib               0x00007fff807dd7fe _dispatch_worker_thread2 + 252
4   libSystem.B.dylib               0x00007fff807dd128 _pthread_wqthread + 353
5   libSystem.B.dylib               0x00007fff807dcfc5 start_wqthread + 13
```

Crash Reporter

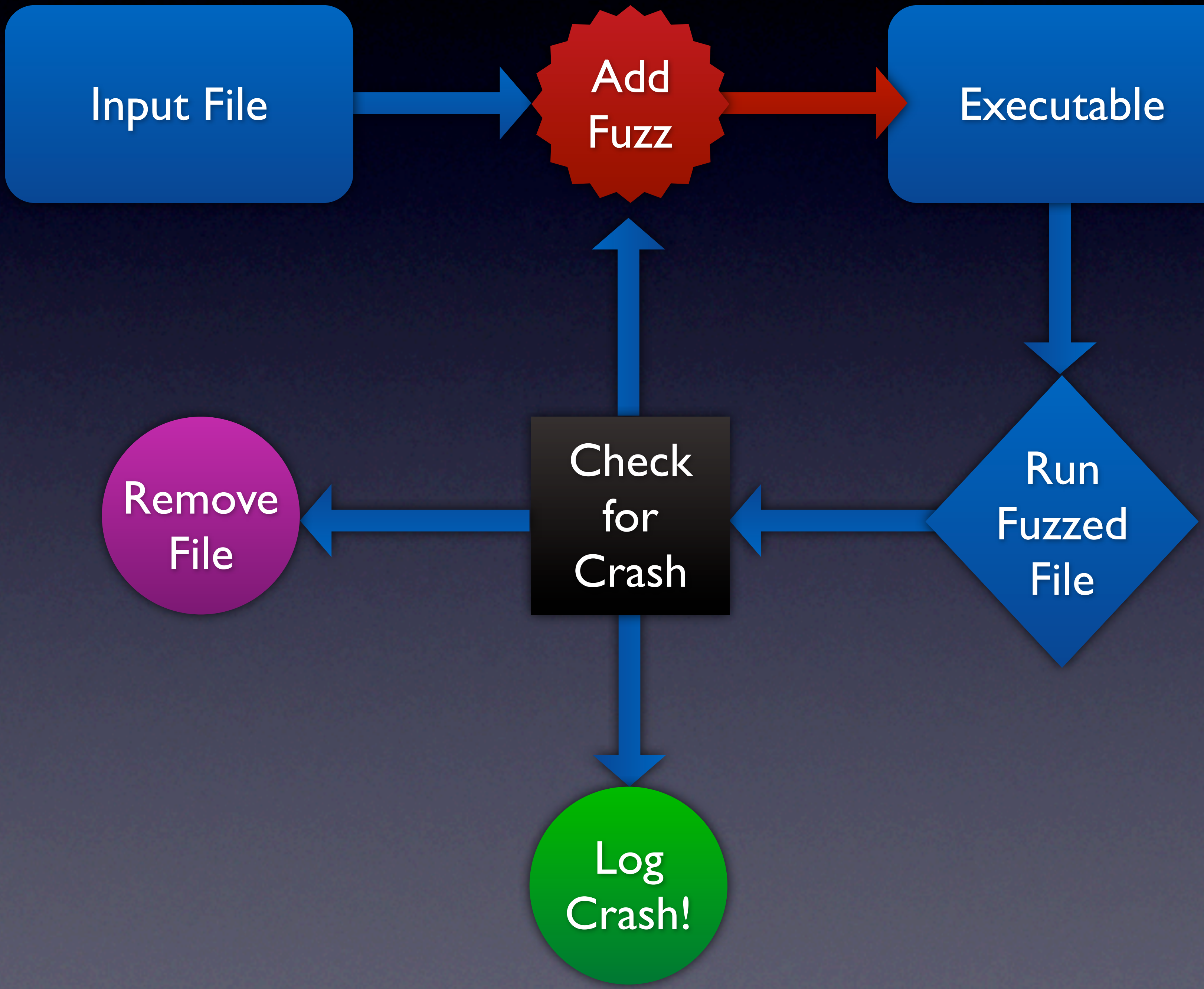


```
0   libSystem.B.dylib                             0x00007fff80824e4e __sigwait + 10
1   libSystem.B.dylib                             0x00007fff80824e27 sigwait + 73
2   libsignals_plugin.dylib                       0x00000001007cf56c SigThread + 124
3   libSystem.B.dylib                             0x00007fff807fc4f6 _pthread_start + 331
4   libSystem.B.dylib                             0x00007fff807fc3a9 thread_start + 13

Thread 3:
0   libSystem.B.dylib                             0x00007fff807fdf8a __semwait_signal + 10
1   libSystem.B.dylib                             0x00007fff80801da1 _pthread_cond_wait + 1286
2   libvlccore.4.dylib                            0x00000001000251c3 libvlc_InternalWait + 51
3   libvlccore.4.dylib                            0x0000000100038d34 MonitorLibVLCDeath + 36
4   libvlccore.4.dylib                            0x00000001000869ee thread_entry + 62
5   libSystem.B.dylib                             0x00007fff807fc4f6 _pthread_start + 331
6   libSystem.B.dylib                             0x00007fff807fc3a9 thread_start + 13

Thread 4:
0   libSystem.B.dylib                             0x00007fff807fdf8a __semwait_signal + 10
1   libSystem.B.dylib                             0x00007fff80801da1 _pthread_cond_wait + 1286
2   libvlccore.4.dylib                            0x0000000100039608 Thread + 120
3   libSystem.B.dylib                             0x00007fff807fc4f6 _pthread_start + 331
4   libSystem.B.dylib                             0x00007fff807fc3a9 thread_start + 13

Thread 5:
0   libSystem.B.dylib                             0x00007fff807fdf8a __semwait_signal + 10
1   libSystem.B.dylib                             0x00007fff807fde19 nanosleep + 148
2   libvlccore.4.dylib                            0x000000010007e58b msleep + 91
3   libmacosx_plugin.dylib                        0x0000000102c0fb89 -[VLCMain manage] + 617
4   libmacosx_plugin.dylib                        0x0000000102c17391 ManageThread + 17
5   libSystem.B.dylib                             0x00007fff807fc4f6 _pthread_start + 331
6   libSystem.B.dylib                             0x00007fff807fc3a9 thread_start + 13

Thread 0 crashed with X86 Thread State (64-bit):
  rax: 0x0000000000000000  rbx: 0x0000000102c79128  rcx: 0x0000000102c79128  rdx: 0x0000000102c6eff0
  rdi: 0x0000000000000000  rsi: 0x0000000000000002  rbp: 0x00007fff5fbff2f0  rsp: 0x00007fff5fbfe6b0
   r8: 0x00007fff5fbff3b8   r9: 0x0000000000000000  r10: 0x00007fff83c20c00  r11: 0x00007fff874e9460
  r12: 0x00007fff84ed6070  r13: 0x00007fff70944422  r14: 0x00000001030a3510  r15: 0x0000000000000000
  rip: 0x000000010008f1bd  rfl: 0x0000000000010202  cr2: 0x0000000000000010
```

Approach

- Select a valid input file
- Select a random fuzzy string from a predefined dictionary
- Run File
  - If the application crashes - get the log
  - If not, delete the file and repeat

Fuzz Flow


Input File
Add Fuzz
Executable
Run Fuzzed File
Check for Crash
Remove File
Log Crash!

Interesting Strings

- The obvious overflow: “...AAAAA...”
- Objective-C
  - %@
  - %p
  - @
  - All C special characters apply too!

Targets

*.flv

*.psd, *.pdf

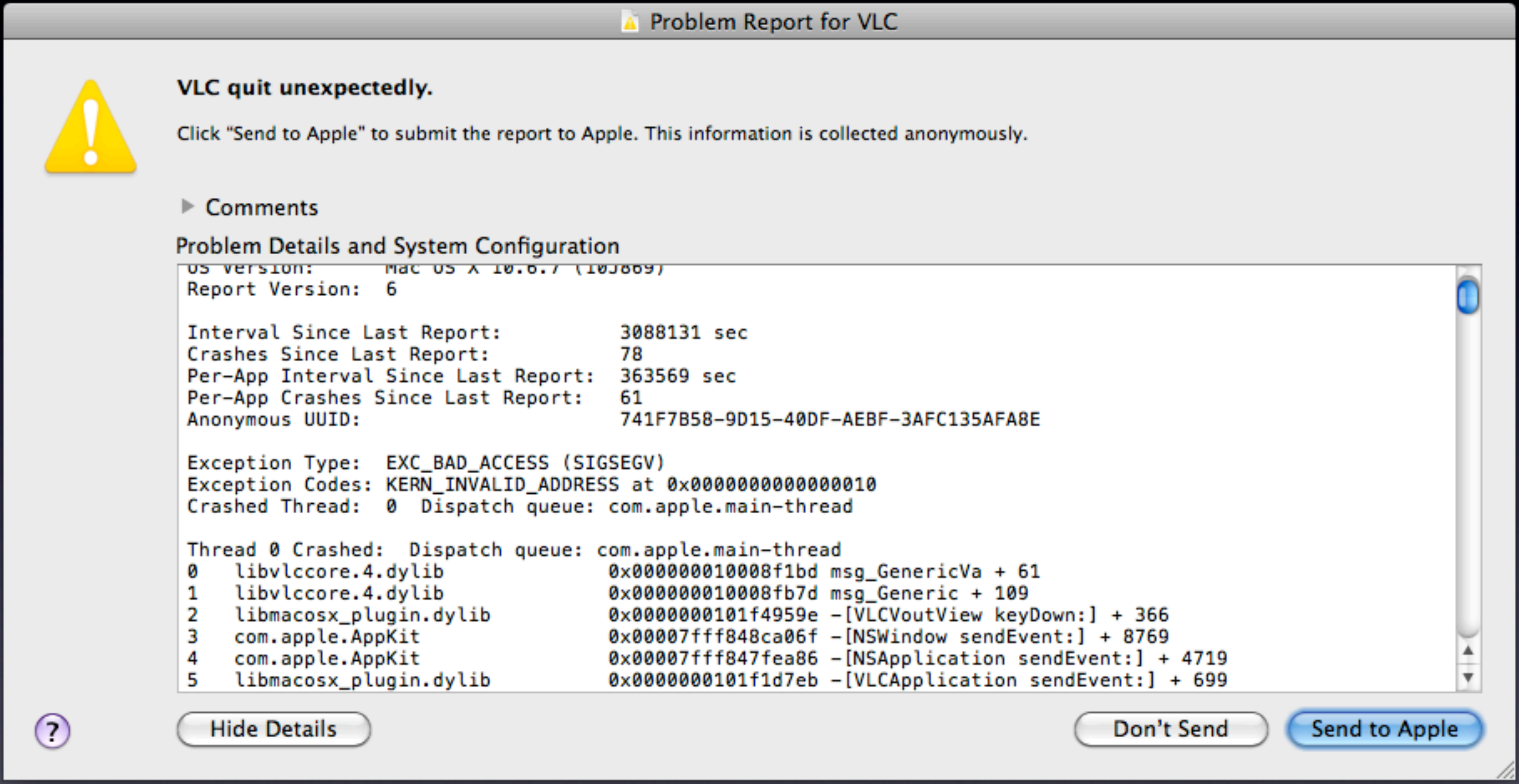
Usage

```
Usage:
python fruityfuzzer.py -a <./path/to/executable>
  -f <./path/to/file> -t <./path/to/directory/for/test/files>
  [options]

 [required]
        -a: Path to Application Executable
        -f: File to seed the Fuzzness
 [options]
        -t: Directory to put the test cases (defaults to ./test/)
        -c: Number of test cases to run (defaults to 1000)
        -T: wait time between trials (default is 5 seconds)
        -v: Verbose
        -h: Help page
```

Results

VLC	Preview
8 Interesting Files Found So Far...	No Interesting Files Found Yet...

VLC Crash



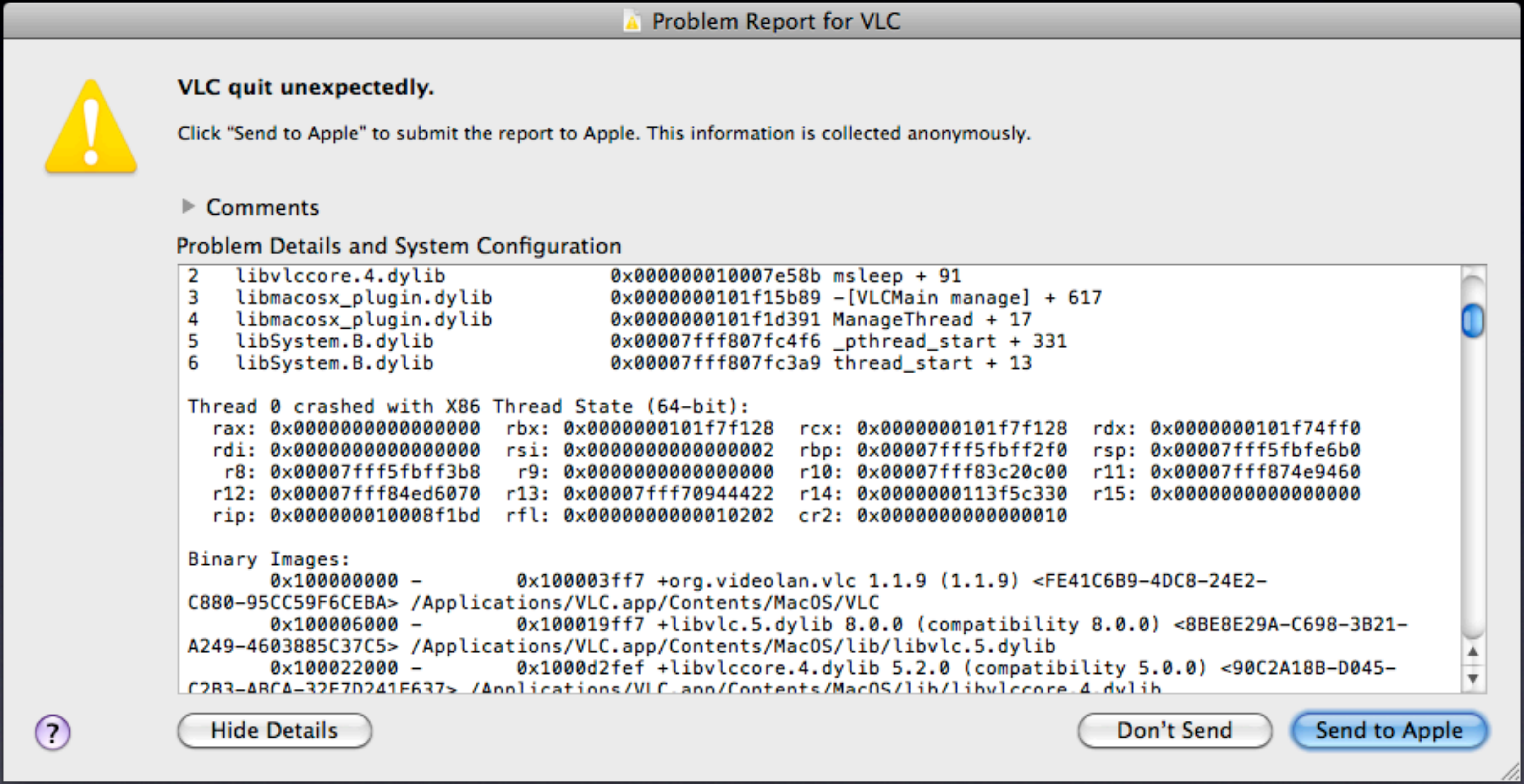
VLC quit unexpectedly.

Click "Send to Apple" to submit the report to Apple. This information is collected anonymously.

Problem Details and System Configuration

```
OS Version:      Mac OS X 10.6.7 (10J869)
Report Version:  6

Interval Since Last Report:          3088131 sec
Crashes Since Last Report:           78
Per-App Interval Since Last Report:  363569 sec
Per-App Crashes Since Last Report:   61
Anonymous UUID:                      741F7B58-9D15-40DF-AEBF-3AFC135AFA8E

Exception Type:  EXC_BAD_ACCESS (SIGSEGV)
Exception Codes: KERN_INVALID_ADDRESS at 0x0000000000000010
Crashed Thread:  0  Dispatch queue: com.apple.main-thread

Thread 0 Crashed:  Dispatch queue: com.apple.main-thread
0   libvlccore.4.dylib              0x000000010008f1bd msg_GenericVa + 61
1   libvlccore.4.dylib              0x000000010008fb7d msg_Generic + 109
2   libmacosx_plugin.dylib          0x0000000101f4959e -[VLCVoutView keyDown:] + 366
3   com.apple.AppKit                0x00007fff848ca06f -[NSWindow sendEvent:] + 8769
4   com.apple.AppKit                0x00007fff847fea86 -[NSApplication sendEvent:] + 4719
5   libmacosx_plugin.dylib          0x0000000101f1d7eb -[VLCApplication sendEvent:] + 699
```

VLC Crash

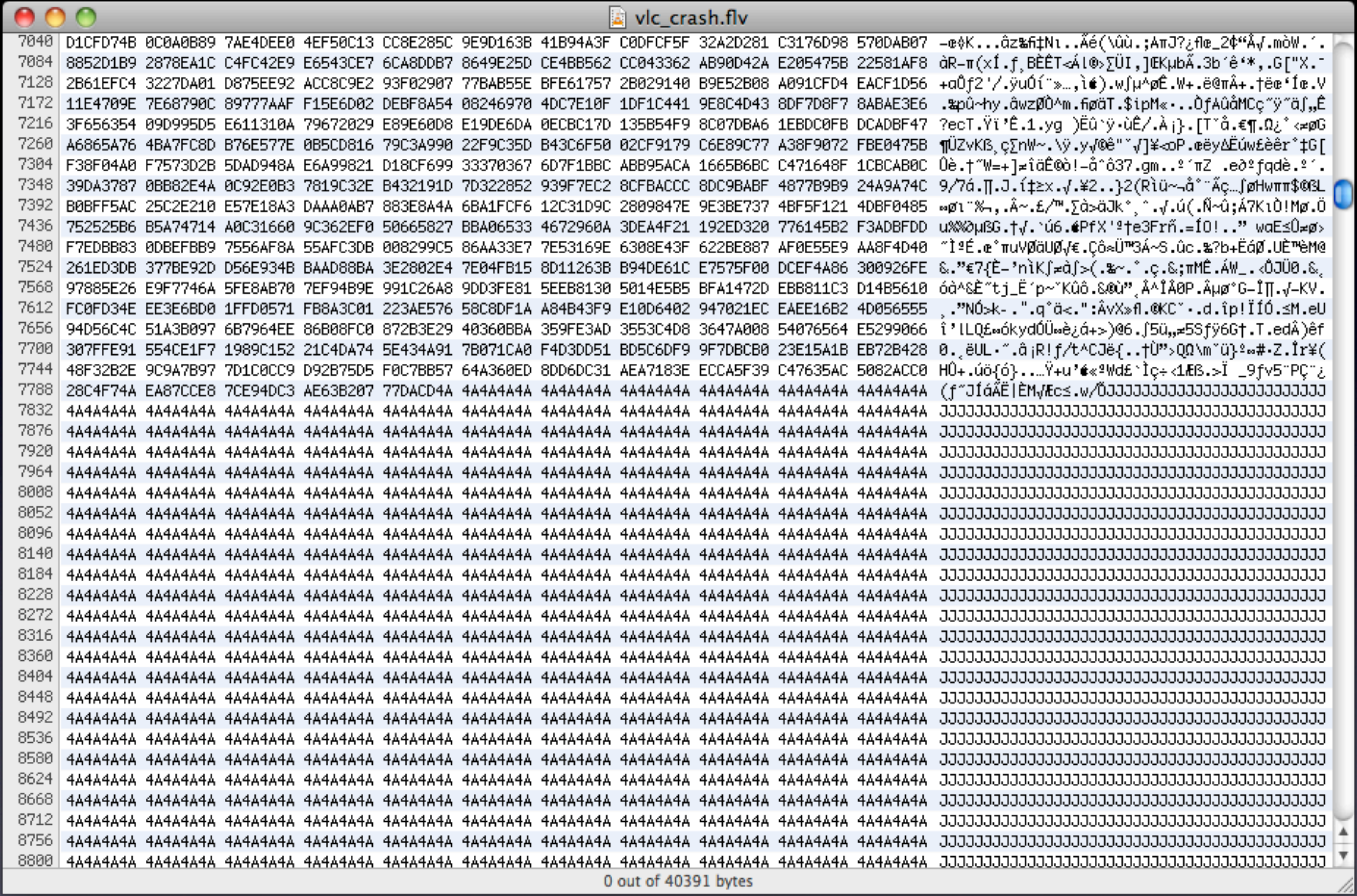


VLC quit unexpectedly.

Click "Send to Apple" to submit the report to Apple. This information is collected anonymously.

Problem Details and System Configuration

```
2   libvlccore.4.dylib              0x000000010007e58b msleep + 91
3   libmacosx_plugin.dylib          0x0000000101f15b89 -[VLCMain manage] + 617
4   libmacosx_plugin.dylib          0x0000000101f1d391 ManageThread + 17
5   libSystem.B.dylib               0x00007fff807fc4f6 _pthread_start + 331
6   libSystem.B.dylib               0x00007fff807fc3a9 thread_start + 13

Thread 0 crashed with X86 Thread State (64-bit):
  rax: 0x0000000000000000  rbx: 0x0000000101f7f128  rcx: 0x0000000101f7f128  rdx: 0x0000000101f74ff0
  rdi: 0x0000000000000000  rsi: 0x0000000000000002  rbp: 0x00007fff5fbff2f0  rsp: 0x00007fff5fbfe6b0
   r8: 0x00007fff5fbff3b8   r9: 0x0000000000000000  r10: 0x00007fff83c20c00  r11: 0x00007fff874e9460
  r12: 0x00007fff84ed6070  r13: 0x00007fff70944422  r14: 0x0000000113f5c330  r15: 0x0000000000000000
  rip: 0x000000010008f1bd  rfl: 0x0000000000010202  cr2: 0x0000000000000010

Binary Images:
       0x100000000 -        0x100003ff7 +org.videolan.vlc 1.1.9 (1.1.9) <FE41C6B9-4DC8-24E2-
C880-95CC59F6CEBA> /Applications/VLC.app/Contents/MacOS/VLC
       0x100006000 -        0x100019ff7 +libvlc.5.dylib 8.0.0 (compatibility 8.0.0) <8BE8E29A-C698-3B21-
A249-4603885C37C5> /Applications/VLC.app/Contents/MacOS/lib/libvlc.5.dylib
       0x100022000 -        0x1000d2fef +libvlccore.4.dylib 5.2.0 (compatibility 5.0.0) <90C2A18B-D045-
C2B3-ABCA-32E7D241E637> /Applications/VLC.app/Contents/MacOS/lib/libvlccore.4.dylib
```



vlc_crash.flv

```
7040 D1CFD74B 0C0A0B89 7AE4DEE0 4EF50C13 CC8E285C 9E9D163B 41B94A3F C0DFCF5F 32A2D281 C3176D98 570DAB07 –œ◊K...âz‰ﬁ‡Nı..Ãé(\ûù.;AπJ?¿ﬂœ_2¢“Å√.mòW.´.
7084 8852D1B9 2878EA1C C4FC42E9 E6543CE7 6CA8DDB7 8649E25D CE4BB562 CC043362 AB90D42A E205475B 22581AF8 àR–π(xÍ.ƒ¸BÈÊT‹Ál®›∑ÜI,]ŒKµbÃ.3b´ê‘*,.G["X.¯
7128 2B61EFC4 3227DA01 D875EE92 ACC8C9E2 93F02907 77BAB55E BFE61757 2B029140 B9E52B08 A091CFD4 EACF1D56 +aÛƒ2'/.ÿuÓí¨»…,ì).w∫µ^øÊ.W+.ë@πÂ+.†ëœ‘Íœ.V
7172 11E4709E 7E68790C 89777AAF F15E6D02 DEBF8A54 08246970 4DC7E10F 1DF1C441 9E8C4D43 8DF7D8F7 8ABAE3E6 .‰pû~hy.âwzØÒ^m.ﬁøäT.$ipM«·..ÒƒAûåMCç˜ÿ˜ä∫„Ê
7216 3F656354 09D995D5 E611310A 79672029 E89E60D8 E19DE6DA 0ECBC17D 135B54F9 8C07DBA6 1EBDC0FB DCADBF47 ?ecT.Ÿï'Ê.1.yg )Ëû`ÿ·ùÊ/.À¡}.[T˘å.€¶.Ω¿˚‹≠øG
7260 A6865A76 4BA7FC8D B76E577E 0B5CD816 79C3A990 22F9C35D B43C6F50 02CF9179 C6E89C77 A38F9072 FBE0475B ¶ÜZvKß¸ç∑nW~.\ÿ.y√®ê"˘√]¥‹oP.œëy∆Ëúw£èêr˚‡G[
7304 F38F04A0 F7573D2B 5DAD948A E6A99821 D18CF699 33370367 6D7F1BBC ABB95ACA 1665B6BC C471648F 1CBCAB0C Ûè.†˜W=+]≠îäÊ®ò!–åˆô37.gm..º´πZ .e∂ºƒqdè.º´.
7348 39DA3787 0BB82E4A 0C92E0B3 7819C32E B432191D 7D322852 939F7EC2 8CFBACCC 8DC9BABF 4877B9B9 24A9A74C 9/7á.∏.J.í‡≥x.√.¥2..}2(Rìü~¬å˚¨Ãç…∫øHwππ$®ßL
7392 B0BFF5AC 25C2E210 E57E18A3 DAAA0AB7 883E8A4A 6BA1FCF6 12C31D9C 2809847E 9E3BE737 4BF5F121 4DBF0485 ∞øı¨%¬,.Â~.£/™.∑à›äJk˚¸ˆ.√.ú(.Ñ~û;Á7KıÒ!Mø.Ö
7436 752525B6 B5A74714 A0C31660 9C362EF0 50665827 BBA06533 4672960A 3DEA4F21 192ED320 776145B2 F3ADBFDD u%%∂µßG.†√.`ú6.PfX'º†e3Frñ.=Í0!..” waE≤Û≠ø›
7480 F7EDBB83 0DBEFBB9 7556AF8A 55AFC3DB 008299C5 86AA33E7 7E53169E 6308E43F 622BE887 AF0E55E9 AA8F4D40 ˜ÌºÉ.œ˚πuVØäUØ√€.Çô≈Ü™3Á~S.ûc.‰?b+ËáØ.UÈ™èM@
7524 261ED3DB 377BE92D D56E934B BAAD88BA 3E2802E4 7E04FB15 8D11263B B94DE61C E7575F00 DCEF4A86 300926FE &.”€7{È–'nìK∫≠à∫>(.‰~.˚.ç.&;πMÊ.ÁW_.‹ÔJÜ0.&¸
7568 97885E26 E9F7746A 5FE8AB70 7EF94B9E 991C26A8 9DD3FE81 5EEB8130 5014E5B5 BFA1472D EBB811C3 D14B5610 óà^&È˜tj_Ë´p~˘Kûô.&®ù”¸Â^ÎÅ0P.Âµø˚G–Î∏.√–KV.
7612 FC0FD34E EE3E6BD0 1FFD0571 FB8A3C01 223AE576 58C8DF1A A84B43F9 E10D6402 947021EC EAEE16B2 4D056555 ¸.”NÓ>k-.".q˚ä<.":ÂvX»ﬂ.®KC˘·.d.îp!ÏÍÓ.≤M.eU
7656 94D56C4C 51A3B097 6B7964EE 86B08FC0 872B3E29 40360BBA 359FE3AD 3553C4D8 3647A008 54076564 E5299066 î'lLQ£∞ókydÓÜ∞è¿á+>)@6.∫5ü„≠5Sƒÿ6G†.T.edÂ)êf
7700 307FFE91 554CE1F7 1989C152 21C4DA74 5E434A91 7B071CA0 F4D3DD51 BD5C6DF9 9F7DBCB0 23E15A1B EB72B428 0.¸ëUL·˜.â¡R!ƒ/t^CJë{..†Ù”>QΩ\m˘ü}º∞#·Z.Îr¥(
7744 48F32B2E 9C9A7B97 7D1C0CC9 D92B75D5 F0C7BB57 64A360ED 8DD6DC31 AEA7183E ECCA5F39 C47635AC 5082ACC0 HÛ+.úö{ó}.……Ÿ+u'«ºWd£`Ìç÷‹1Æß.>Ï _9ƒv5¨PÇ¨¿
7788 28C4F74A EA87CCE8 7CE94DC3 AE63B207 77DACD4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A (ƒ˜JÍáÃË|ÈM√Æc≤.w/ÕJJJJJJJJJJJJJJJJJJJJJJJJJ
7832 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
7876 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
7920 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
7964 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8008 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8052 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8096 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8140 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8184 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8228 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8272 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8316 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8360 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8404 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8448 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8492 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8536 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8580 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8624 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8668 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8712 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8756 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
8800 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A 4A4A4A4A JJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJJ
```

0 out of 40391 bytes

Drawbacks

- Fuzzer doesn’t understand code coverage
- Fuzzer isn’t aware of protocols or formats
- Dependent on Platform being up to date
- No Debugging Mode
- Serial flow

Future Work

- Add multithreading support
- Port *pydbg.py* to python 2.7 and OS X 10.6 for full debugging functionality
- More robust reporting
- Smarter Trials
  - Protocol Aware

References

- “The Mac Hacker's Handbook,” Charlie Miller, Dino Dai Zovi
- http://code.google.com/p/sulley/
- http://peachfuzzer.com
- http://cansecwest.com/csw08/csw08-miller.pdf
- http://developer.apple.com/library/mac/#documentation/Cocoa/Conceptual/Strings/Articles/formatSpecifiers.html