Whitepaper:

Software Forensics (or: What Can I Do After the Lights Go Out?)



Introduction

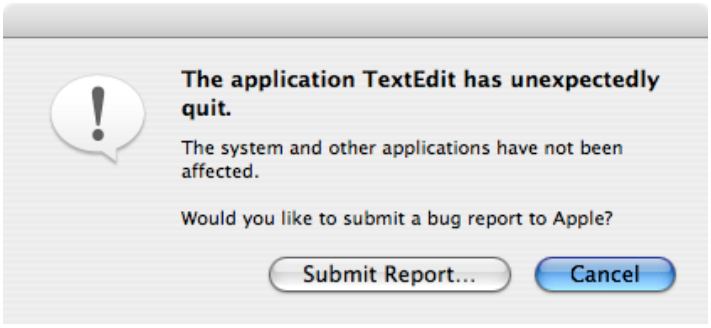
Nobody likes crashes—and nobody likes the inevitable questions that follow: “what were you doing?” “What was the last thing you did before it crashed?” “Were you doing anything different?”

Fortunately, Mac OS X records quite a bit of information about your system whenever a crash happens, and this information can be a major help to the programmers who are trying to track it down. This is a guide to help you help us find the bugs we all want to get rid of!

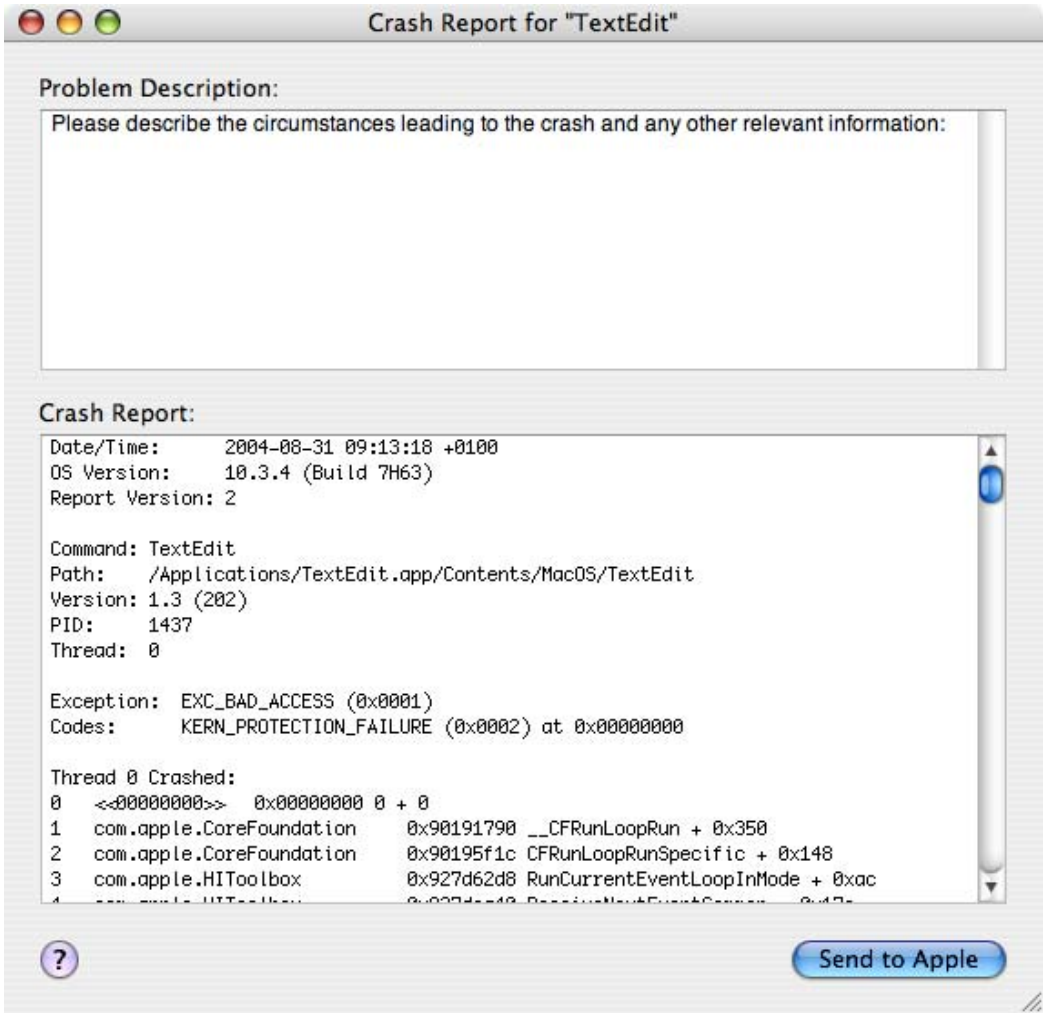
The first question is: what kind of crash was it? In general, there are three kinds of crashes in Mac OS X: application crashes, kernel panics, and startup crashes. The following guide will help you identify which type of crash you have and where to find additional information that was logged by the system.

Application Crash:

An Application Crash is one where a specific application stops running, but other applications continue to run and (in most cases) you can re-launch the original application and continue working. The system usually announces that an Application Crash has occurred by displaying the following dialog:



The first thing to note is the name of the application that crashes. In most circumstances this will be the application you are currently using - but sometimes it may be another application that is running in the background. If you click on the “Submit Report…” button, you'll be shown a second dialog with information on the state of the application when it ran into problems, like this:

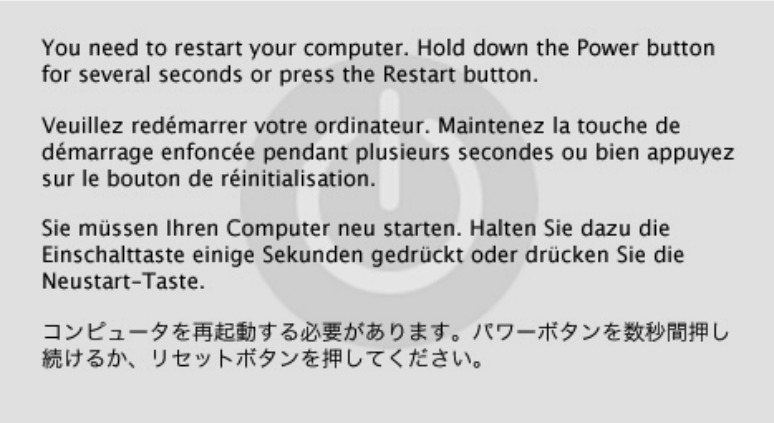


While it may look like gibberish, the information in the “Crash Report:” box is valuable stuff to programmers. Apple developed the Crash Reporter tool to make it easy to send crash information back to their developers, but if you suspect that AJA software might be involved (or just need help confirming it), you can copy the contents of the Crash Log box to the clipboard (the window acts like any text processing application), paste it into an e-mail and send it to us. The Crash Report dialog can be dismissed without sending a copy to Apple by clicking on the red “close” button in the upper-left corner of the window. Note: don't send the report to Apple unless you are sure that their software is the problem!

What if you've already dismissed the Crash Report dialog and want to get it back or compare it with previous crashes? OS X keeps copies of each crash report in a directory called “Crash Reporter”, located in your User/Library/Logs directory. You will find files for every application that has experienced a crash, e.g. “Final Cut Pro.crash.log”. If you're not sure what application was running when the crash occurred, check the “Date Modified” and look for the most recent date. The crash log files are plain TEXT files that can be opened with any text processor—the default is the Console application provided by Apple. They records cumulative events of every crash: you'll find the most recent incident at the bottom of the document.

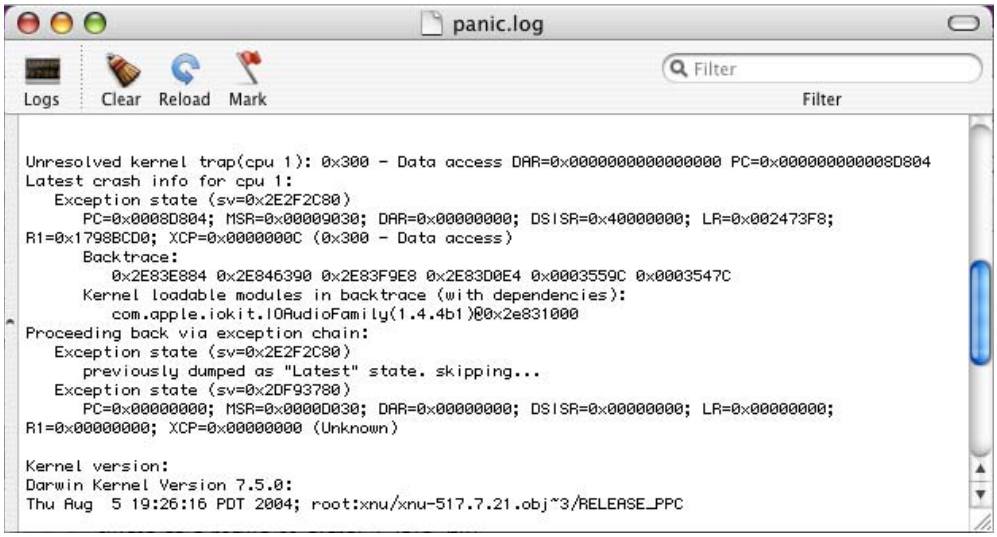
Kernel Panics:

Kernel panics happen when the software that is failing is running in the most privileged “kernel” level of the operating system. A kernel crash is usually announced by your Mac going dark and the following screen appearing:



The only way “out” of this kind of crash is to shut down the computer and restart it. While there is no way for the OS to display a “Crash Reporter” dialog, it still saves some valuable information in a file called “panic.log”, located in the /Library/logs directory (note that this is the top-level “Library” folder, not the User/Library folder where you previously found the Crash Reporter files).

The “panic.log” file is also a plain TEXT file which defaults to opening in the Console application. It also records crash information cumulatively, so the most recent information will be at the bottom. An example looks something like this:



This text may also be copied and pasted into an e-mail or other text document, or the entire file can be attached to an e-mail.

Startup Crashes:

Startup crashes are ones that happen while your computer is booting (i.e. following a power-on or restart), and leaves the computer dead or "frozen" before it can display the initial login window or your user desktop. Technically this is just a form of an application or kernel crash that happens before the system is alive enough to show you a Crash Report. Fortunately the system saves the same CrashReport information in .log files - but usually in a different location.

Because the crash usually happens before a user has logged in, the crash reports are saved in the /Library/logs directory (same as the panic.log file above). However, to get to the files you first have to be able to boot the computer! Here are two hints for getting running again:

First, restart the computer (you'll probably have to press and hold the Power button until the Mac shuts off, then press it again to restart it). Immediately hold the keyboard SHIFT key down until the computer has successfully launched. Holding the SHIFT key down tells OS X to only load the minimum number of system extensions it needs to operate. Since we're pretty sure they worked once, there is a good chance that your computer should work with them again. This means that some peripherals that have been added on top of the basic OS will not load (including KONA drivers) in this mode.

Once you have successfully booted, you can look for clues in the /Library/log Crash reporter files (check the modification dates for the most recent), or in the "system.log" file. The "system.log" file is used by the OS and some peripherals to log important messages - and in some cases you may find an indication of a warning or error message from some device. To access the system.log file, open the Console application (located in /Applications/Utilities), go to the File menu and select "Open System log". The system log is also cumulative (if you've had your computer for awhile it may be quite large!), and the most recent information is at the bottom of the file. All messages are time and date-stamped so you can look for ones that happened just before the time you had the problem. Messages from the System log can also be copied and pasted into an e-mail.

A second technique for troubleshooting Boot Crashes is to boot in "Verbose" mode. To do this, start the computer and immediately hold down the "command" (aka "Apple") and "V" keys at the same time. You can let go after the initial gray screen with the Apple logo has disappeared and lots of text has started to appear on your screen.

What you'll see is the same text that is going into the system.log file, and if there is a hang-up or a crash you may be able to see it as it is happening. You won't be able to cut and paste the contents of the screen - but it can give you an immediate indication of what went wrong.

Other Useful Information:

In tracking down bugs, it's also very useful for us to know the hardware configuration of your system. The easiest way to get that is by using the Apple System Profiler application, found in your /Applications/Utilities directory. When you launch System Profiler, it examines the hardware and software setup from your computer and distills it into a single report. The report can be saved as an XML ".spx" file which can be attached to an e-mail, or it can be Exported as a Plain Text file which can then be attached or copy/pasted into the body of an e-mail. You can choose the type of report (Short/Standard/Extended) from the application's "View" menu. For most uses, the "Short Report" is sufficient.

Note: all reports print a considerable amount of information about the software you have installed and your computer's operating configuration. We highly recommend reviewing the report before sending it to us (or anyone else) to make sure that there is no sensitive information in it that you do not want to share. If so, Export the report as a text file and edit out the information you don't want to share.

Another source of information specific to your KONA installation is the Info tab in the Kona Control Panel application. This lists some pertinent information about your hardware, as well as a list of the Kona software modules installed on your system. The text information from this window may be copy/pasted into an e-mail application and included with any bug reports.