

microsoft.public.development.device.drivers: Re: How to read current kernel image from driver?

## Re: How to read current kernel image from driver?

**Source:**

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2004-04/1242.html>

---

**From:** Doug Phelps (*Doug4361\_at\_hotmail.com*)

**Date:** 04/23/04

Date: 22 Apr 2004 17:14:54 -0700

I guess I need to refine my question somewhat. All I need to know is how I can best determine the object path to the currently active kernel image on disk. The best I can come up with now is to try read environment variables once the system is up to determine the DosDevices path, but that's cheesy.

There has got to be a simple way to determine the path to the current kernel's image file.

Anyone know what it is?

Thanks,  
Doug

"Doron Holan [MS]" <doronh@nospam.microsoft.com> wrote in message news:<eqyFMGIKEHA.3920@TK2MSFTNGP10.phx.gbl>...

> *how can you verify integrity given that service packs and hotfixes can  
> legitimately change the code that you are supposed verifying? \SystemRoot  
> is a valid start to a path, you can figure out how to get the rest i am  
> sure.*

>

> d

>

> --

> *This posting is provided "AS IS" with no warranties, and confers no rights.*

> *Please reply to newsgroups only.*

>

> *"Doug Phelps" <Doug4361@hotmail.com> wrote in message*

> *news:86940cce.0404220658.4211d9fe@posting.google.com...*

> > *I want to be able to read parts of the current kernel' image on disk*

> > *from a driver. This is partly to verify integrity of the current*

> > *kernel.*

> >

> > *I'm having problems with this. First, I can't determine current*

> > *kernel.*

> >

> > *NtQuerySystemInformation provides me with*

microsoft.public.development.device.drivers: Re: How to read current kernel image from driver?

> > "*\\WINNT\System32\ntoskrnl.exe*" as a path, but how do I convert that to  
> > useable path for *ZwOpenFile* or *ZwCreateFile*? This has to work for  
> > kernels that have been renamed or load from non-c: drives.  
> >  
> > This also assumes that the first entry returned in the module  
> > information list is always the kernel image, which may be a bad  
> > assumption.  
> >  
> > I'm not even certain that I can then read the file if I open it. I'd  
> > want to open, read, and close the file during my *DriverEntry*.  
> >  
> > Any advice?  
> >  
> > Thanks  
> > -Doug