

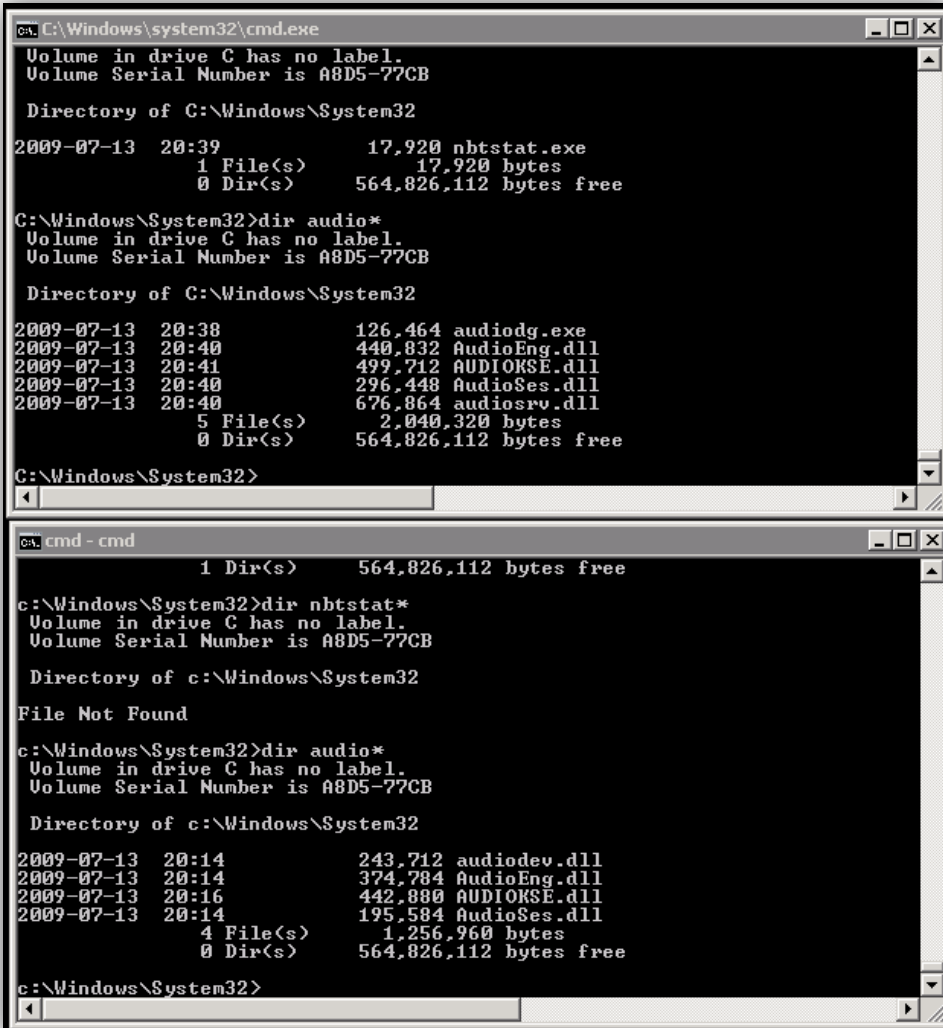
## FINDING NBSTAT UTILITY ON 64-BIT SYSTEM (WINDOWS 7)

### SCENARIO

*A while back I tried to use nbtstat on my 64bit Windows 7 machine and it seemed to not be installed. Well, I did some more research into this. After a while I figured out that if I launched a command prompt using the usual shortcut I had been using, nbtstat would not be found.*

*But if I launched cmd.exe from the start menu, it could be found. When listing the contents of the system32 directory the files were different when depending how I launched the command line.*

Here is a single screen shot of two command prompts. The directory commands were executed within seconds of each other. The top command prompt can see **nbtstat.exe**, but it cannot see **audiodev.dll**. The bottom command prompt cannot see **nbtstat.exe**, but can see **audiodev.dll**.



```
C:\Windows\system32\cmd.exe
Volume in drive C has no label.
Volume Serial Number is A8D5-77CB

Directory of C:\Windows\System32

2009-07-13  20:39                17,920 nbtstat.exe
             1 File(s)                17,920 bytes
             0 Dir(s)                564,826,112 bytes free

C:\Windows\System32>dir audio*
Volume in drive C has no label.
Volume Serial Number is A8D5-77CB

Directory of C:\Windows\System32

2009-07-13  20:38                126,464 audiodg.exe
2009-07-13  20:40                440,832 AudioEng.dll
2009-07-13  20:41                499,712 AUDIORKSE.dll
2009-07-13  20:40                296,448 AudioSes.dll
2009-07-13  20:40                676,864 audiosrv.dll
             5 File(s)                2,040,320 bytes
             0 Dir(s)                564,826,112 bytes free

C:\Windows\System32>

cmd - cmd
             1 Dir(s)                564,826,112 bytes free

c:\Windows\System32>dir nbtstat*
Volume in drive C has no label.
Volume Serial Number is A8D5-77CB

Directory of c:\Windows\System32

File Not Found

c:\Windows\System32>dir audio*
Volume in drive C has no label.
Volume Serial Number is A8D5-77CB

Directory of c:\Windows\System32

2009-07-13  20:14                243,712 audiodev.dll
2009-07-13  20:14                374,784 AudioEng.dll
2009-07-13  20:16                442,880 AUDIORKSE.dll
2009-07-13  20:14                195,584 AudioSes.dll
             4 File(s)                1,256,960 bytes
             0 Dir(s)                564,826,112 bytes free

c:\Windows\System32>
```

Looking at these closely, did you notice that the times on the files displayed on both command prompts were different?

The gotcha here is how Windows handles launching 32 bit programs on a 64 bit system. Many of us have probably noticed the “**Program Files**” directory is for 64 bit programs and the “**Program Files (x86)**” directory is for the 32 bit programs. The **system32** directory is for 64 bit programs and DLLs and there is a **sysWOW64** directory for the 32 bit **system32** files.

But instead of the operating system just activating the correct **DLL** when a program needs it, it does some sneaky root kit like work. Here is what is really going on:

When running a 32 bit program, the **sysWOW64** directory looks like the **system32** directory so no matter what the program does, it cannot try to load a **64 bit DLL**. Or it cannot even load a 64 bit executable. I was launching the command prompt by using a shortcut. But I was launching it from a 32 bit program launcher.

A 32 bit program can launch a 64 bit program if it can find it. But when my 32 bit program launcher went looking for **cmd.exe** in the **system32** directory, it actually found the 32 bit **cmd.exe** in the **sysWOW64** directory and just didn't know it.

So **Windows 7** does not come with a 32 bit **nbtstat**, only the 64 bit version. So that is why I could not find **nbtstat**.