

# Sure, we do that

---

 [devblogs.microsoft.com/oldnewthing/20040211-00](http://devblogs.microsoft.com/oldnewthing/20040211-00)

February 11, 2004



Raymond Chen

The DirectX video driver interface for Windows 95 had a method that each driver exposed called something like “DoesDriverSupport(REFGUID guidCapability)” where we handed it a capability GUID and it said whether or not that feature was supported.

There were various capability GUIDs defined, things like GUID\_CanStretchAlpha to ask the driver whether it was capable of stretching a bitmap with an alpha channel.

There was one driver that returned TRUE when you called DoesDriverSupport(GUID\_XYZ), but when DirectDraw tried to use that capability, it failed, and in a pretty spectacular manner.

So one of the DirectDraw developers called the vendor and asked them, “So does your card do XYZ?”

Their response: “What’s XYZ?”

Turns out that their driver’s implementation of DoesDriverSupport was something like this:

```
BOOL DoesDriverSupport(REFGUID guidCapability)
{
    return TRUE;
}
```

In other words, whenever DirectX asked, “Can you do this?” they answered, “Sure, we do that,” without even checking what the question was.

(The driver must have been written by the sales department.)

So the DirectDraw folks changed the way they queried for driver capabilities. One of the developers went into his boss’s office, took a network card, extracted the MAC address, and then smashed the card with a hammer.

You see, this last step was important: The GUID generation algorithm is based on a combination of time and space. When you ask CoCreateGuid to create a new GUID, it encodes the time of your request in the first part of the GUID and information that uniquely

identifies your machine (the network card's MAC address, which is required to be unique by the standards that apply to network card).

By smashing the network card with a hammer, he prevented that network card from ever being used to generate a GUID.

Next, he added code to DirectDraw so that when it starts up, it manufactures a random GUID based on that network card (which – by its having been destroyed – can never be validly created) and passes it to DoesDriverSupport. If the driver says, “Sure, we do that”, DirectDraw says, “Aha! Caught you! I will not believe anything you say from now on.”

Raymond Chen

**Follow**

