

Project 9x: Using WinDbg on a Crash Dump from gogoCLIENT (10 pts.)

What You Need

- A Windows 7 machine (real or virtual), with WinDbg installed, and the Microsoft Symbols installed, as you did in the previous project.

Warning!

Your machine may need Startup Repair after this project. Don't use a machine you love, or one that isn't backed up.

If you don't have an expendable machine, use the S214 lab machines.

Purpose

Using WinDbg to analyze a crash dump.

Installing the gogoCLIENT

Click **Start**, "**Control Panel**", "**Uninstall a Program**".

If there is any version of the gogoCLIENT installed, remove it first. This bug only works on a fresh install.

Download and install the gogoCLIENT Utility version 1.0-RELEASEHACCESSwin32 from this link:

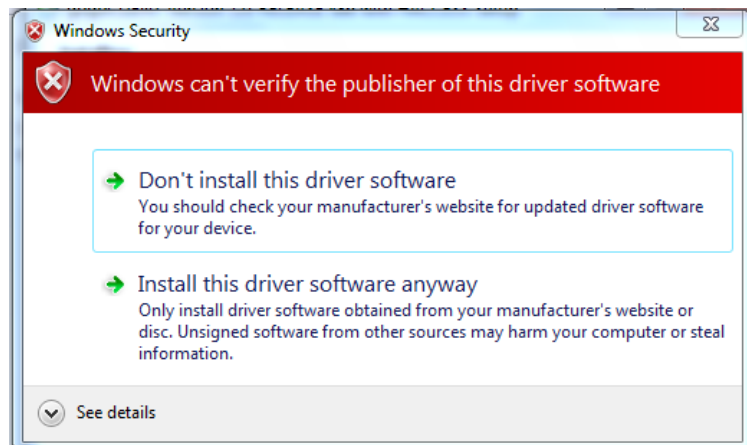
[gogoc1.0RELEASEHACCESSwin32.exe](#)

This utility allows you to make IPv6 connections through Freenet6, but that's not important for this project.

The useful thing for this project is that it has a serious bug (it was fixed in later versions).

During the installation, you will see this scary warning box, suggesting that this driver is unsafe, which is correct.

Click "**Install this driver anyway**".



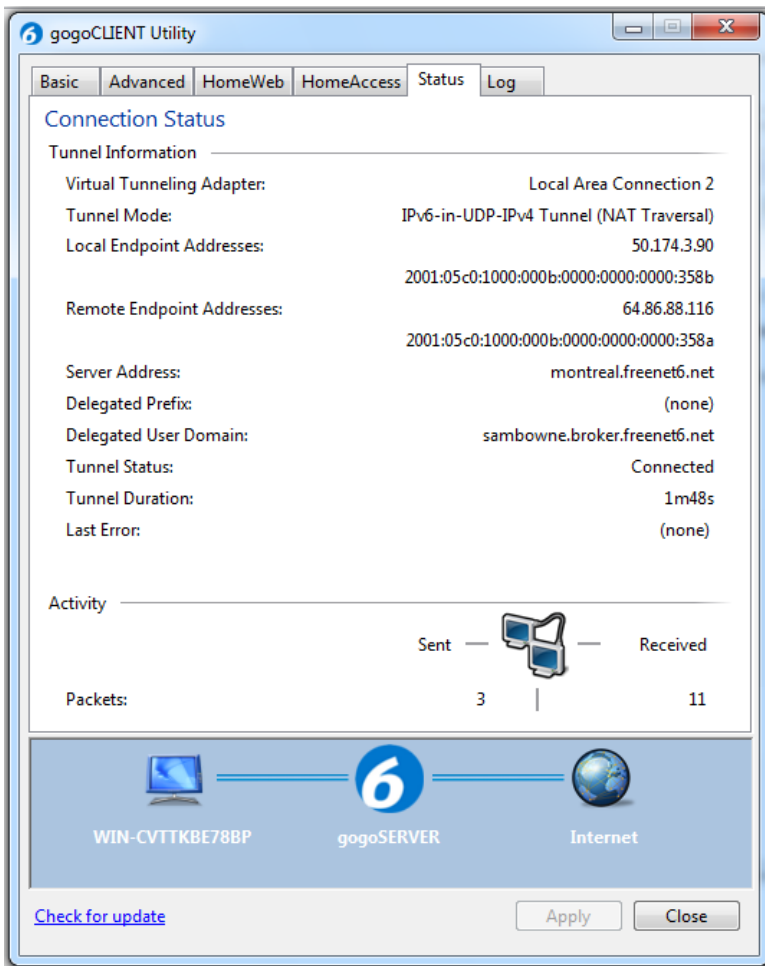
Running the gogoCLIENT

Run the client.

In the "gogoCLIENT Utility" box, on the **Basic** tab, click the **Connect** button.

Click the **Status** tab and wait until it connects. as shown below.

NOTE: this is not possible on the CCSF wireless network, because the port is blocked. You can use the wired network in S214, however.



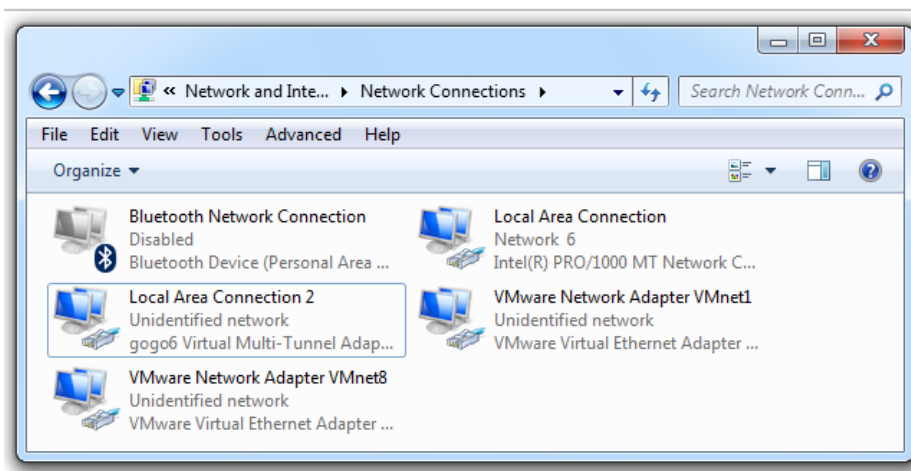
Causing a Blue Screen Error

Click **Start**.

Type in **CONNECTIONS**

Click "**View network connections**".

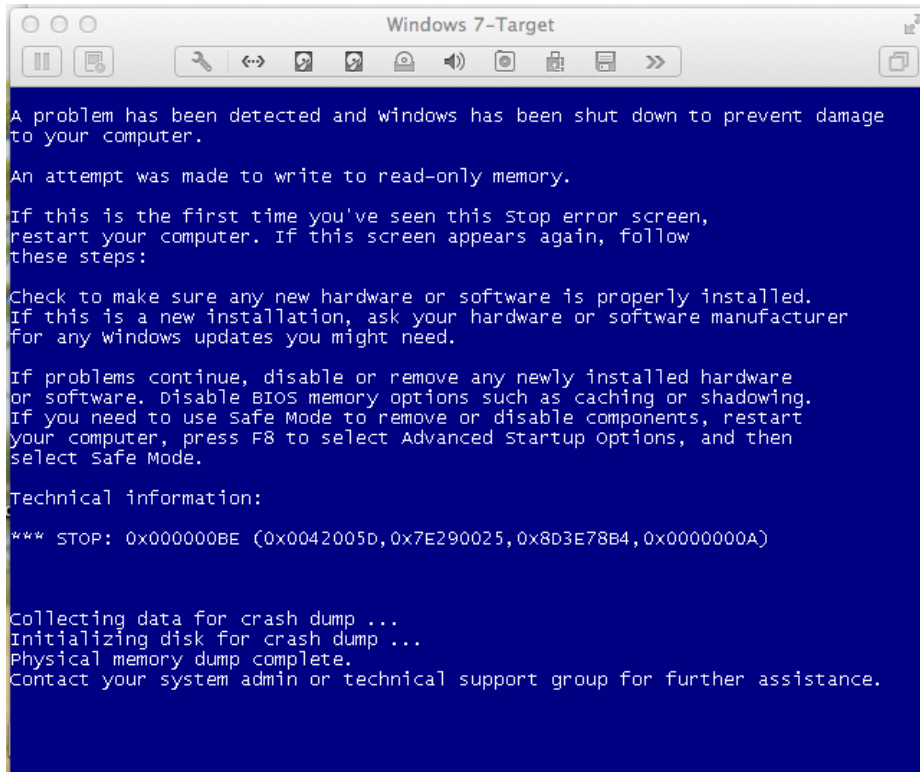
In the Network Connections window, find the "**gogo6 Virtual Multi-Tunnel Adapter**", as shown below.



Right-click the the "**gogo6 Virtual Multi-Tunnel Adapter**" and click **Disable**.

In the gogoCLIENT window, on the **Basic** tab, click **Disconnect**.

You should see the Blue Screen of Death, as shown below:



Wait till you see the message "Physical memory dump complete", as shown above. Power the machine off.

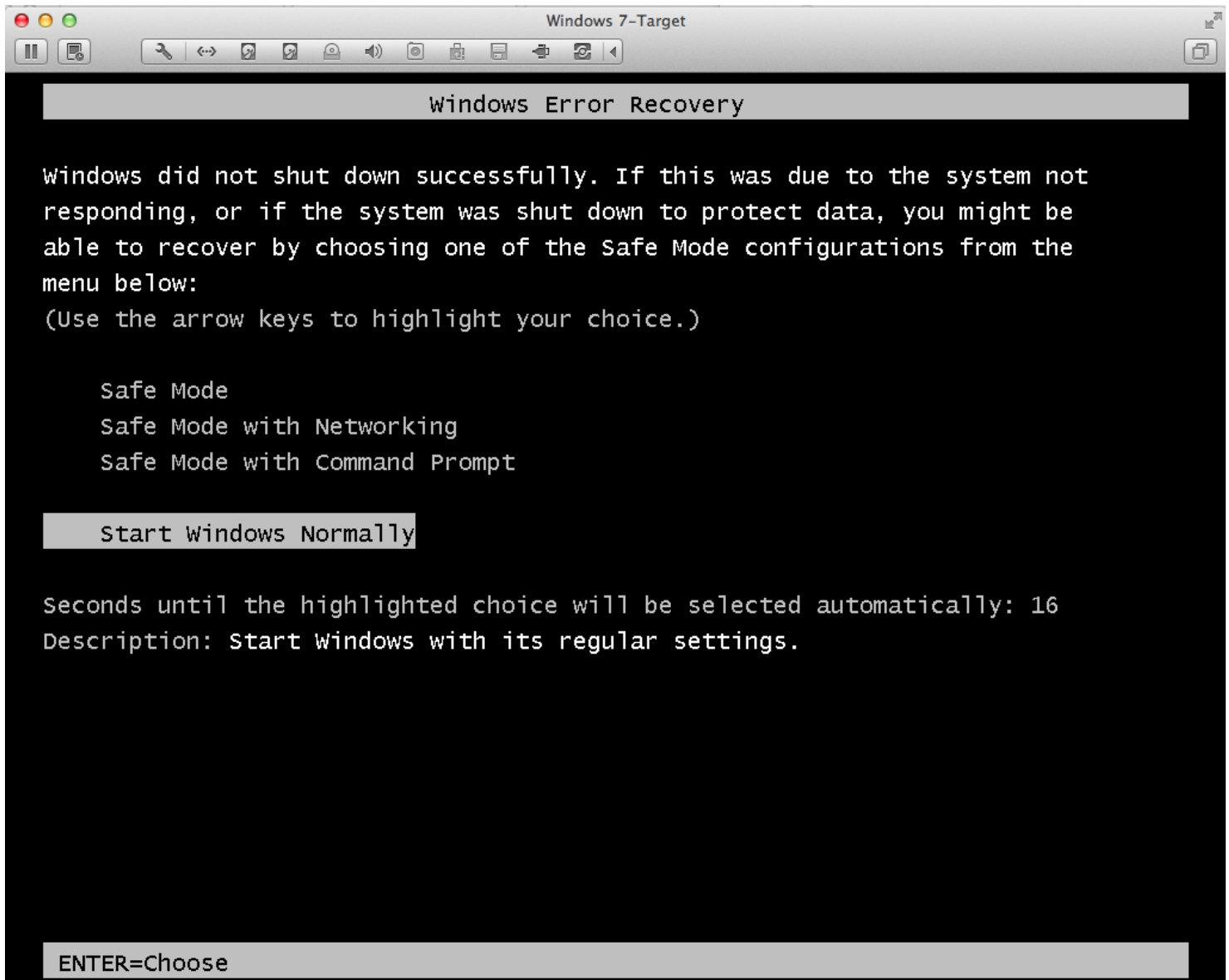
If you are using a virtual machine, click "**Virtual Machine**", "**Shut Down**", "**Force Shut Down**", "**Force Shut Down**".

Restarting your Machine

Power your Windows machine on again.

The "Windows Error Recovery" screen appears, as shown below.

Highlight "**Start Windows Normally**" and press **Enter**.

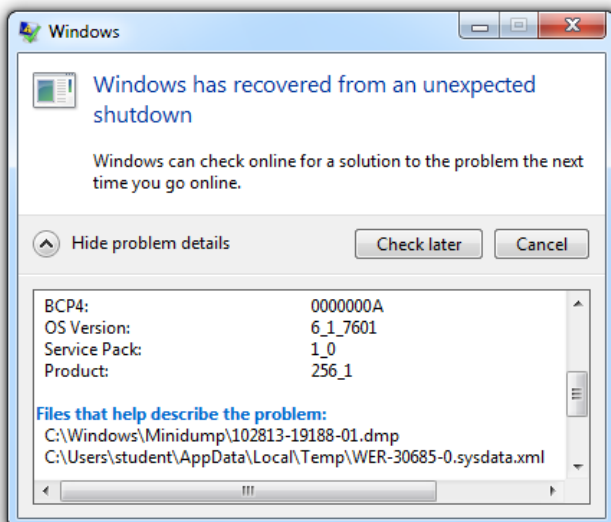


Note: Sometimes I was unable to restart Windows this way, and I had to run "Startup Repair" twice.

When the machine starts again, you see a box saying "**Windows has recovered from an unexpected shutdown**", as shown below.

Click the "**View problem details**" arrow and scroll down to find the filename of the crash dump file.

In the example below, the crash dump file is "C:\Windows\Minidump\102813-19188-01.dmp".



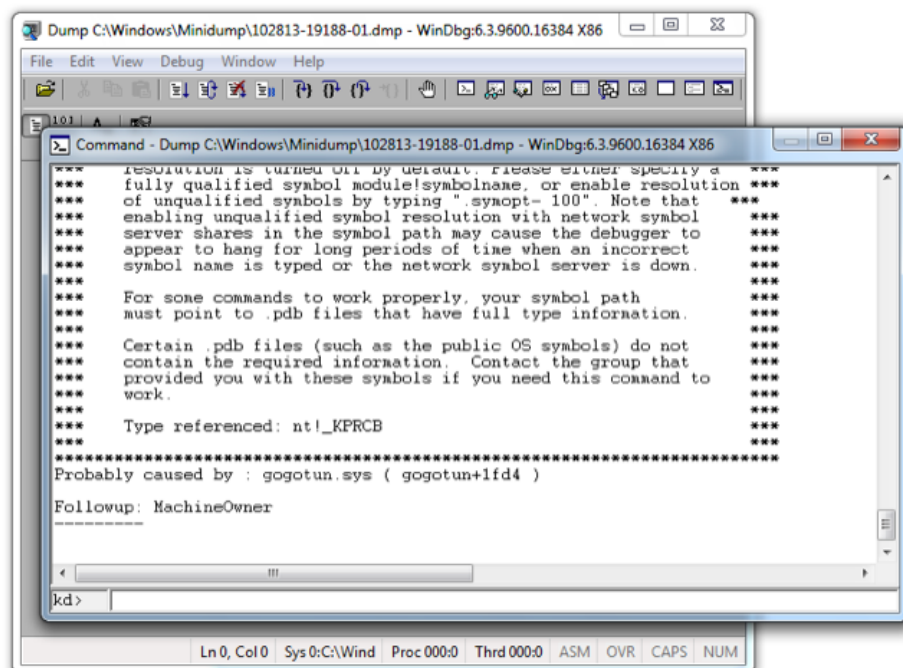
Analyzing the File in WinDbg

Start WinDbg as administrator.

Configure the symbol path, as you did before.

Open the dump file.

At the bottom, you see the message "**Probably caused by gogotun.sys**", as shown below.



```
Dump C:\Windows\Minidump\102813-19188-01.dmp - WinDbg:6.3.9600.16384 X86
File Edit View Debug Window Help
*** resolution is turned on by default. Please either specify a ***
*** fully qualified symbol module!symbolname, or enable resolution ***
*** of unqualified symbols by typing ".sympath- 100". Note that ***
*** enabling unqualified symbol resolution with network symbol ***
*** server shares in the symbol path may cause the debugger to ***
*** appear to hang for long periods of time when an incorrect ***
*** symbol name is typed or the network symbol server is down. ***
***
*** For some commands to work properly, your symbol path ***
*** must point to .pdb files that have full type information. ***
***
*** Certain .pdb files (such as the public OS symbols) do not ***
*** contain the required information. Contact the group that ***
*** provided you with these symbols if you need this command to ***
*** work. ***
***
*** Type referenced: nt!_KPRCB ***
*****
Probably caused by : gogotun.sys ( gogotun+1fd4 )
Followup: MachineOwner
-----
kd>
```

Saving a Screen Image

Make sure you can see the message "**Probably caused by gogotun.sys**", as shown above.

Save a whole-desktop image with a filename of "**Proj 9x from YOUR NAME**".

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT.

Turning in Your Project

Email the image to: cnit.126sam@gmail.com with a subject line of **Proj 9x From Your Name**, replacing Your Name with your own first and last name. Send a Cc to yourself.

Last Modified: 10-28-13 3:26 pm