

Re: Problem with matching kind of NDIS driver.

Re: Problem with matching kind of NDIS driver.

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2007-07/msg00226.html>

- *From:* "Witoslaw Jozewicz" <wj78[NoSpaM](at)wp.pl>
 - *Date:* Tue, 10 Jul 2007 20:31:56 +0200
-

"mirage2k2" <mirage2k2@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:E5F3B882-1DD7-45A2-909D-97DC4E02FECD@xxxxxxxxxxxxxxxxxxxx

With TDI driver and NDIS IM you can match traffic to PID via port number only. What does your driver really need to do? If you need to queue

That is them of my Master of Science Job, I have to find a way how to solve that problem on NDIS driver layer.

packets then you must use NDIS IM driver. If you just want to sniff/modify packets then there are some other options, i.e. filter hook, etc. Note also that you will not see any packets in the TDI driver, rather you see IOCTLs for operations such as connect, send, receive, etc. Filtering such commands will allow you to obtain PID/TID, port numbers and for some, remote ip addresses. Mirage2k2

I need a driver which will catch all packets going through network card, find PID's for that, and sends all the informations for application on users layer (that application will be logging all network activities – it has to work as the "netstat -anb" application but in real time). Thanks for your advices, Mirage2k2.

—
With regards
thanks,
Witek

.