

Q: Tracing TCP/IP print jobs for analysis of data and protocols - need a tool.

Question:

I need to trace a TCP/IP print job in order to analyze the data and protocols. The commercially available "sniffers" are very expensive, and I might not be sure that the format can be read by the Intermate support department, should I need to send it in for analysis. Can you recommend a tool?

Answer:

Many Intermate print servers include trace function. If you are working with IPDS products such as the IAPS IPDS and the WinIPDS, we recommend the IPDSCapture Tool (P22).

If the trace function provided does not meet all your needs, or if you are using a product with no built-in trace function, we recommend the freely available sniffer tool Wireshark (formerly known as **Ethereal**).

Wireshark can be downloaded from this web site: <http://www.wireshark.org> and is available for several operating systems including Windows. The website includes instructions on migrating from Ethereal, which it replaces as of June 2006.

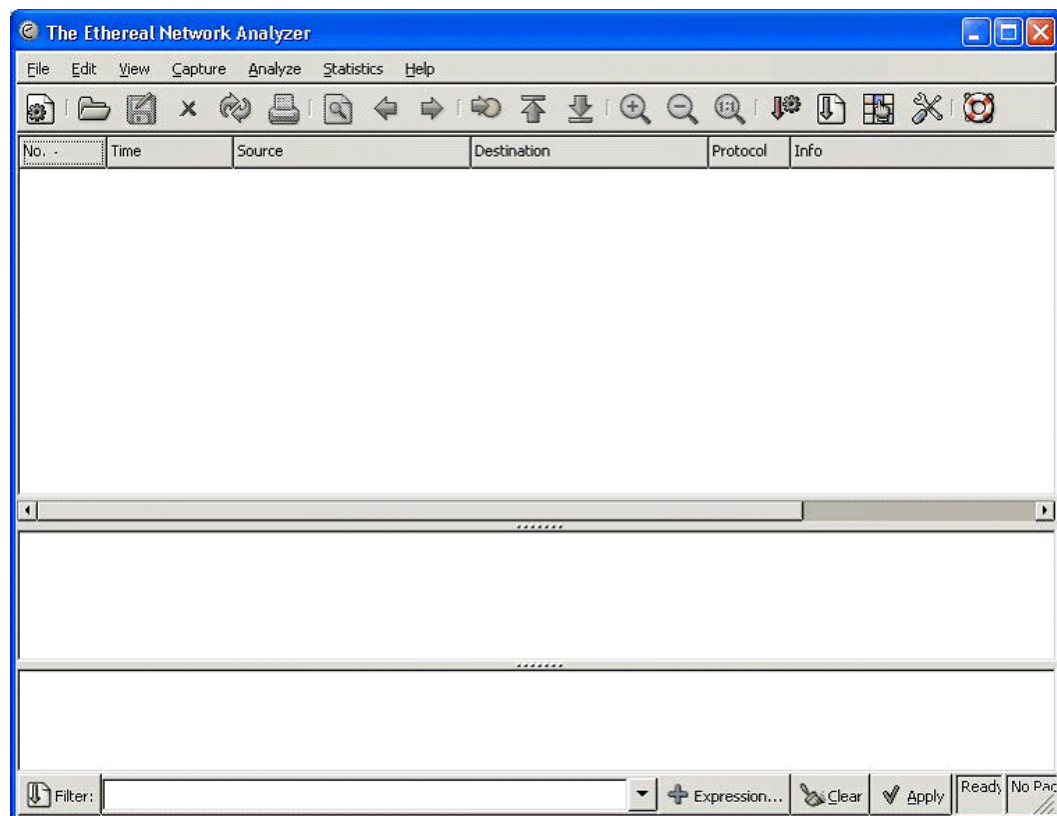
Important:

Make sure you are sitting on the same subnet as the printer you want to trace. If two separate physical networks are involved, it is recommended to install a HUB between the printer and the network and connect the trace PC to the same HUB (a switch may not work).

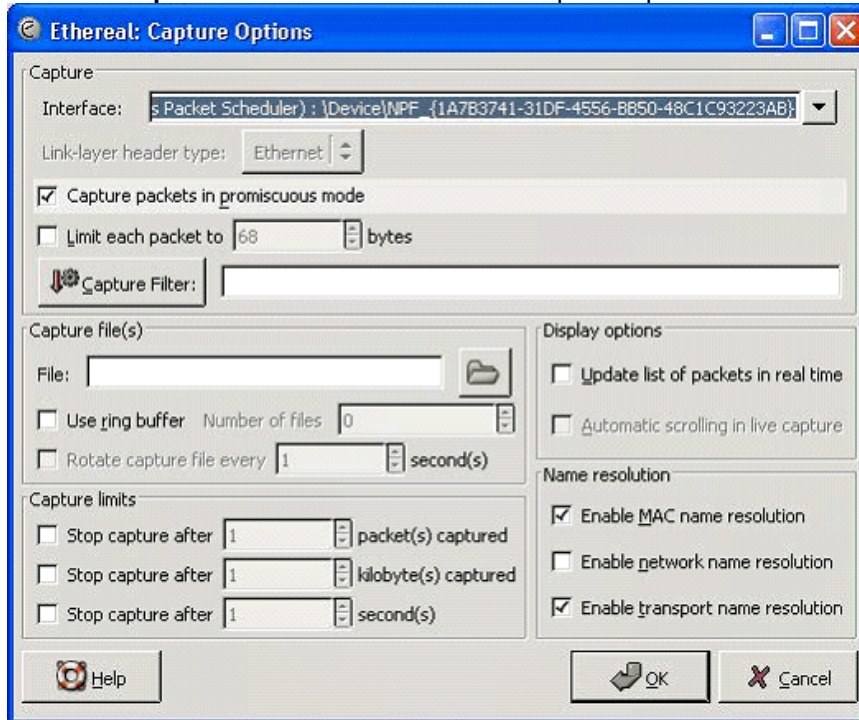
How to create a capture

The example below shows Ethereal version 0.10.2; the Intermate print server is the Intermate Advanced Print Server (IAPS) - IPDS. Screen shots were last updated in January 2005, so they may not be completely up to date.

1. Start Ethereal, Result:



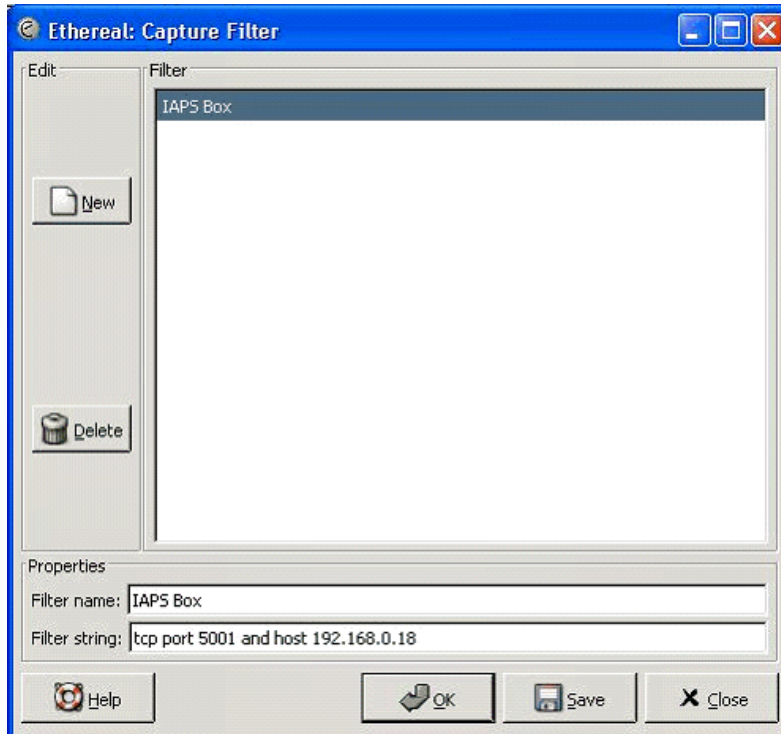
2. Select **Capture > Start**. The result is the Capture Options screen.



3. Make sure that the correct NIC is selected in the **Interface** field in the Capture Options screen above.

4. Click the **Capture Filter** button. The result is the Capture Filter screen.

The screen shot below shows the result after you have followed the steps to create a new filter.



5. To create a new filter on the Capture Filter screen:

a) In the Properties area of the screen (bottom area of Capture Filter, type in a **filter name**, e.g. IAPSBox as shown above - or IPDStrace01 - or whatever you find helpful.

b) Type in a **filter string**

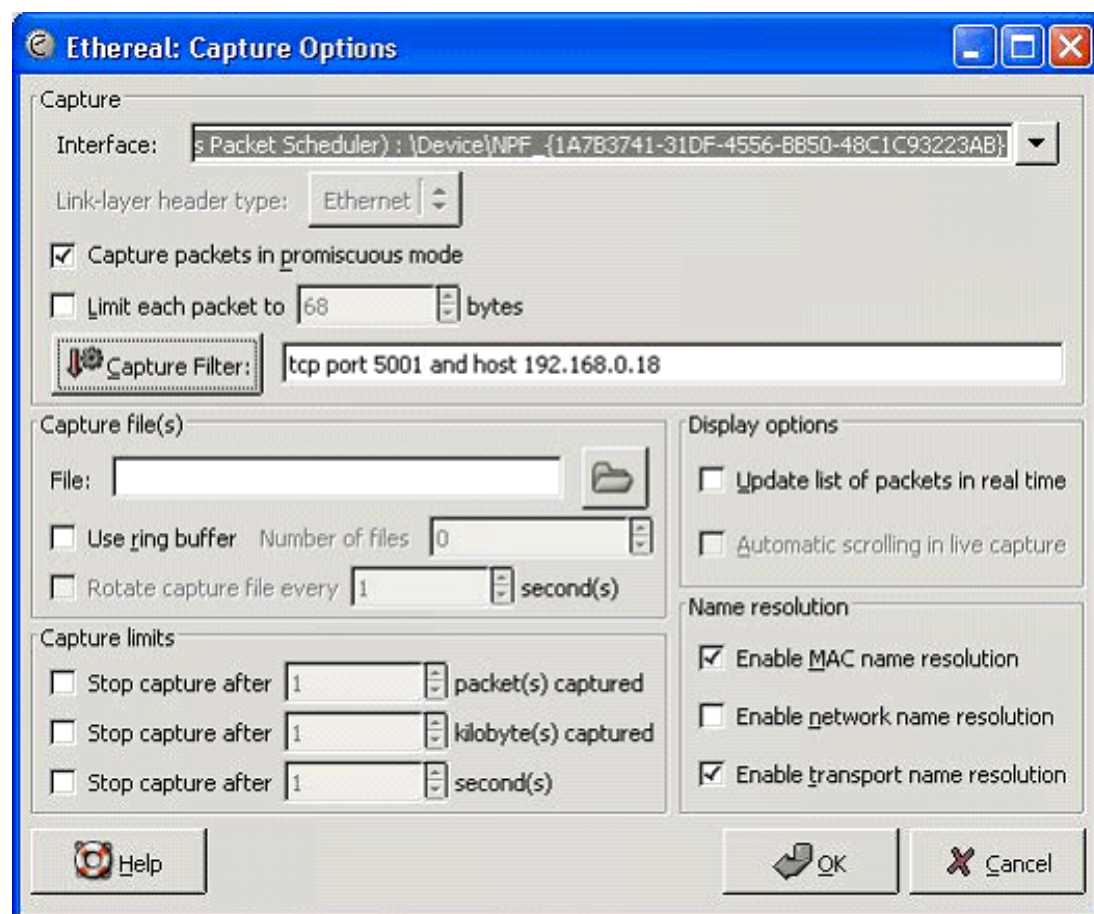
Even though you can use Display filters, it is usually a good idea to use Capture filters in order to make the trace file as small as possible. In the example above, a filter is given on a port and a host IP address.

The IP address that you give for the "host" part of the string - in this example 192.168.0.18 - is that of the "device" you want to sniff. (Device is a generic term for printer and print server).

If you know the actual TCP port data is transmitted on, you can narrow the trace to by entering the appropriate printer port. For example, for Raw Socket data only (PCL, PS), this would probably be tcp port 9100, and the string would look like this: "tcp port 9100 and host 192.168.0.18". The example above uses tcp port 5001, a very commonly used IPDS port. But remember, the actual port may have a different number.

c) Click **New** to add the filter to the list, then **Save** and then **OK**.

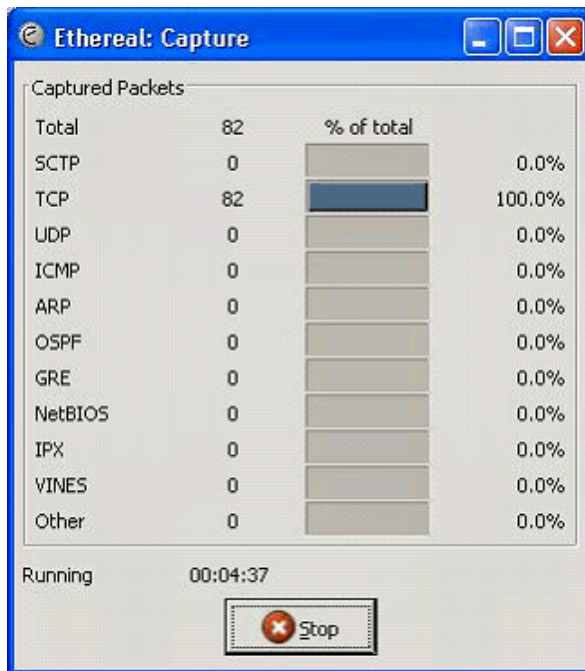
d) Result: You are back on the **Capture Options** view.



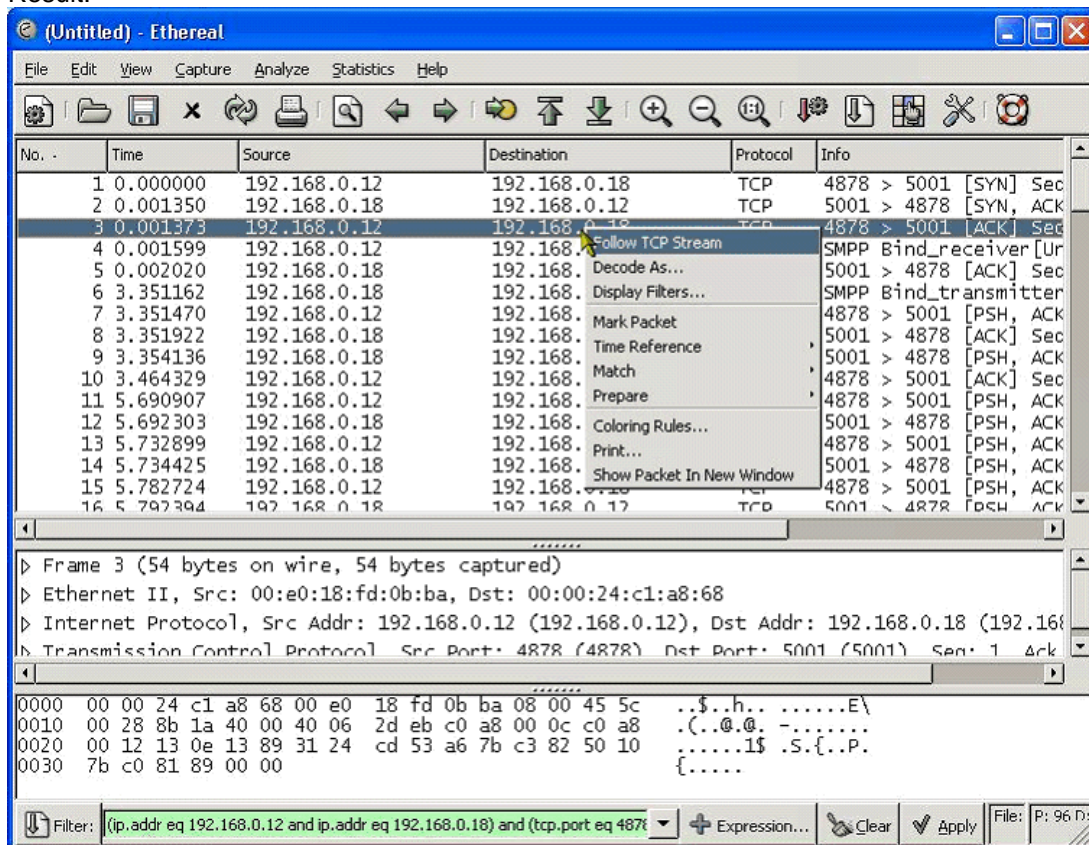
6. To **start the capture**, click **OK** (bottom right on Capture Options.).

7. Power on the "device" that you want to sniff and submit the host print job.

8. While the capture is running, Ethereal keeps track of the **status with the Capture screen**: The screen dump below shows a trace lasting 4 minutes and 37 seconds, capturing 82 tcp packets.



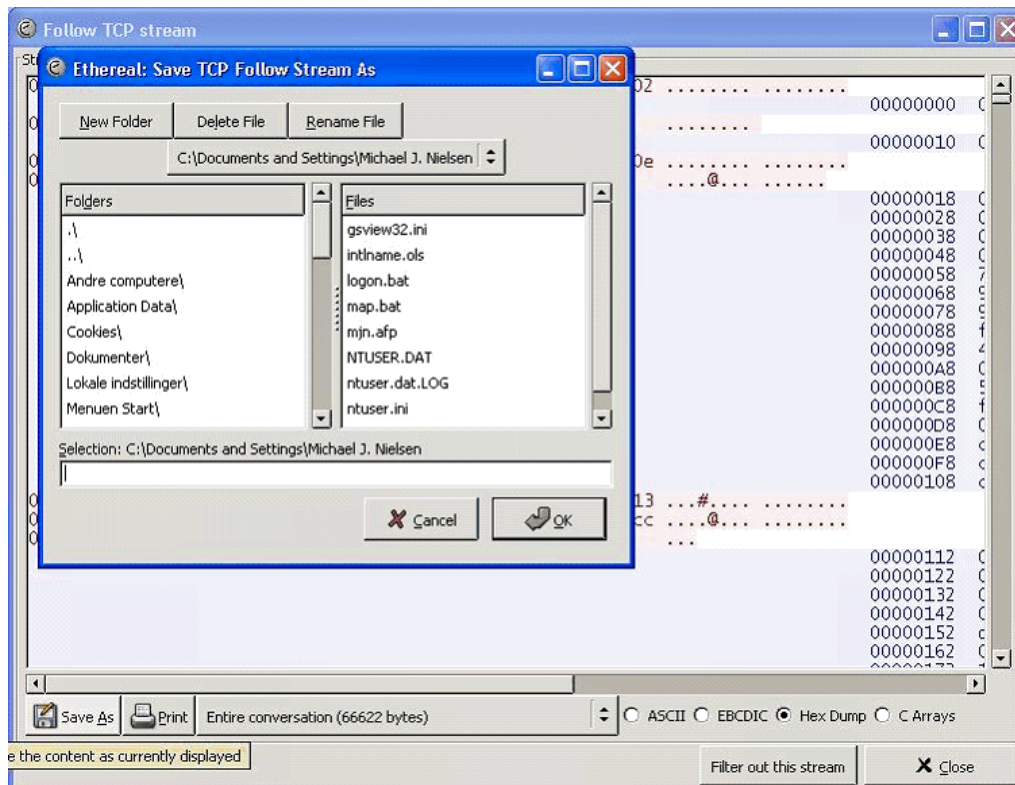
9. When the print job is finished, click the Stop button on the Ethereal: Capture screen. Result:



10. To examine the result

Right Click on a stream with the desired IP address and Port and select **Follow TCP Stream** from the context menu. Result (back window only on the screen shot below). As you can see, the capture file is in Hex format.

11. To save the result: Click on "Save As" (bottom left). This opens the foreground window on the screen shot below. Name the file and click OK.



Updated 13 January 2005; 28 September 2007.