Steps to capture Wireshark network trace to aid troubleshooting

For issues reported for AS/400 systems printing to Lexmark laser devices.

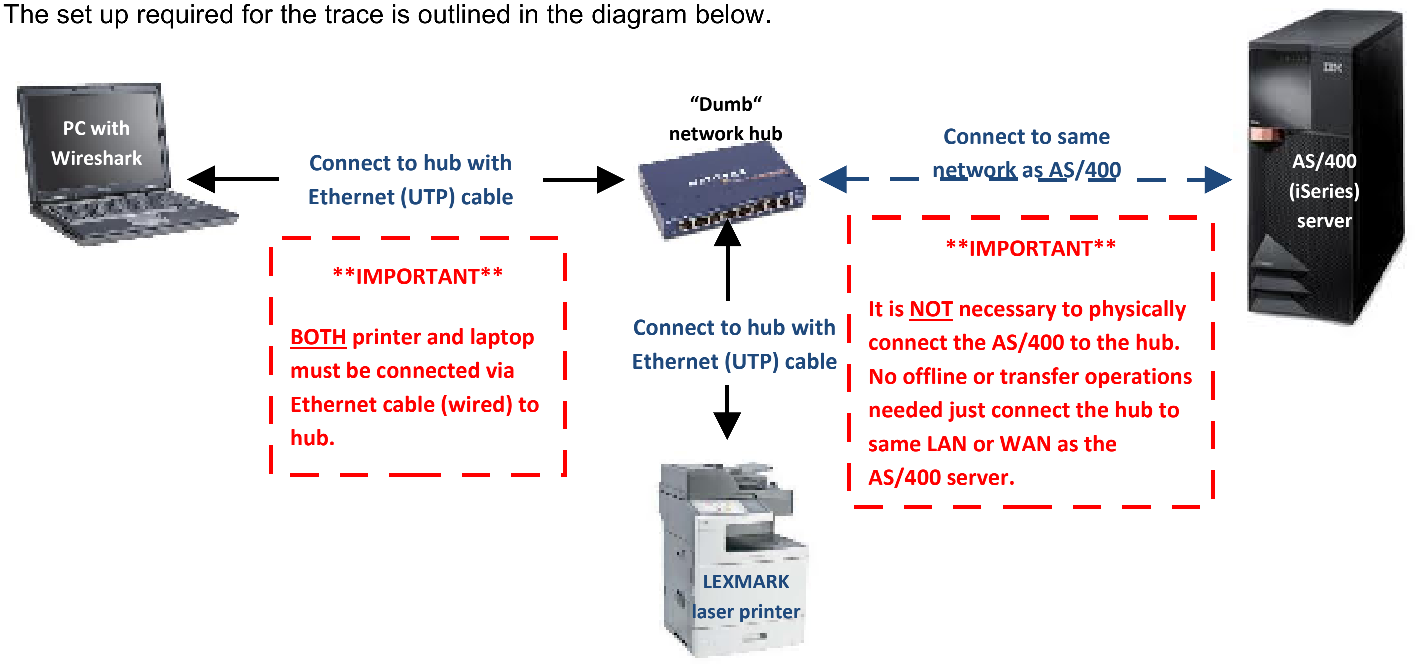
NOTE: Sample host commands included are based on V6R1 and specific only to AS/400 systems. Users can use this document as a general guide for gathering Wireshark traces but will need to request for host commands specific to their systems if they are working with non-AS/400 systems such as z/OS mainframes or Infoprint servers.

This document basically covers three major steps.

1. Preparing the setup
2. Gathering the trace
3. Verifying the trace

Step 1: Prepare correct trace setup

The set up required for the trace is outlined in the diagram below.



IMPORTANT

BOTH printer and laptop must be connected via Ethernet cable (wired) to hub.

IMPORTANT

It is NOT necessary to physically connect the AS/400 to the hub. No offline or transfer operations needed just connect the hub to same LAN or WAN as the AS/400 server.

1a. Prepare Requirements

Only requires two (2) additional elements to the customer's usual setup:

1. PC or laptop with Wireshark installed

2. A network hub. Not a switch, not a router, but the older and "dumber" network hub.

If laptop does not have Wireshark installed, please download the open source application from http://www.wireshark.org/download.html. This document uses screen shots from Wireshark v1.2.1.

It is important to use a network hub instead of a switch or router to enable Wireshark to monitor the communication between printer and host.

1b. Set Up Connection

The printer will need to be attached to the hub and will be offline for a few minutes to allow the re-routing of connection. The printer should be back online once connected to the hub. To facilitate transfer, please attach the hub to the network first.

1. Connect the network hub to the same network as the AS/400 server.

2. Connect printer or printers to be tested to the network hub using an Ethernet (UTP) cable.

3. Connect laptop with Wireshark to the network hub using an Ethernet (UTP) cable.

Take note that there is no need to disconnect the AS/400 from the network AT ALL during this setup.

1c. Validate Setup

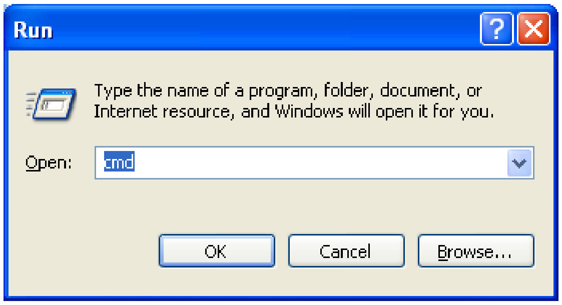
1. Make sure the network hub, PC and printer are powered ON.

2. Make sure the printer has a valid IP address. This can be verified by printing the menu settings from **`Menus > Reports > Network Setup Page`**, or by going to **`Menus > Network/Ports > Standard Network > Std Network Setup > TCP/IP`**

3. Make sure the laptop can communicate with printer.

    a. Ping the printer from the laptop's command line.

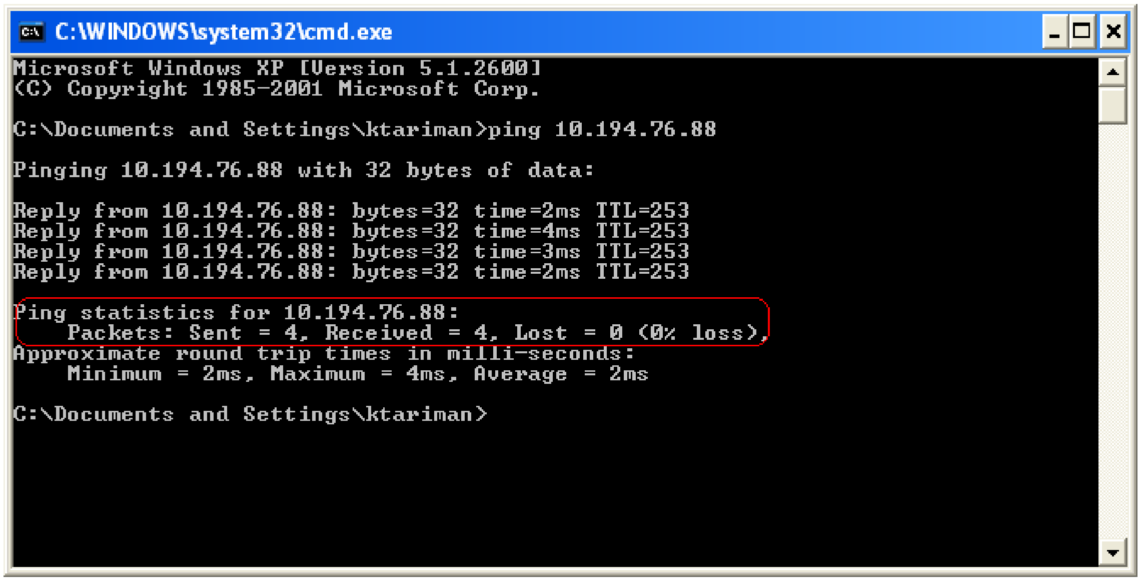
        i. Go to **`Start > Run`** then input **`cmd`** then press Enter or click on OK to launch the DOS command prompt.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

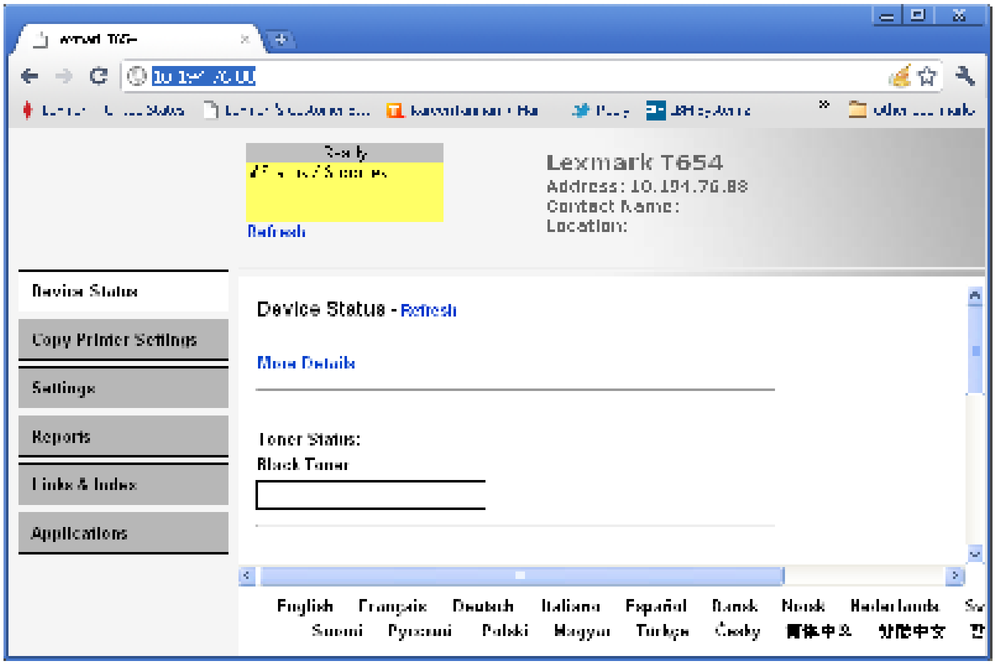
Open: cmd

ii. On the command line, input `ping 'printer's ip address'` and wait for response. There should be no data loss.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ktariman>ping 10.194.76.88

Pinging 10.194.76.88 with 32 bytes of data:

Reply from 10.194.76.88: bytes=32 time=2ms TTL=253
Reply from 10.194.76.88: bytes=32 time=4ms TTL=253
Reply from 10.194.76.88: bytes=32 time=3ms TTL=253
Reply from 10.194.76.88: bytes=32 time=2ms TTL=253

Ping statistics for 10.194.76.88:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\Documents and Settings\ktariman>
```

b. Or access the printer's EWS page by opening a browser and inputting the printer's IP address from step 2.


Ready
Refresh
Device Status
Copy Printer Settings
Settings
Reports
Links & Index
Applications
More Details
English Français Deutsch Italiano Español Dansk Norsk Nederlands
Suomi Русский Polski Magyar Türkçe Česky

Lexmark T654
Address: 10.194.76.88
Contact Name:
Location:

Device Status - Refresh

Toner Status:
Black Toner

4. Make sure the AS/400 can still print to the printer. Run a test job.

    a. If the AS/400 is unable to print, have the AS/400 operator make sure that the IP address on the Device Description is the same as the IP address gathered in step 2. IP may have changed when printer was re-attached to network. If IP address is different, change it to the one currently used by the printer.

5. Once setup is verified, then you are read to start gathering the trace. Proceed to step 2.

Step 2: Gather the trace

To perform this step, the user must:

2a. Stop the printer writer on AS/400

2b. Start the Wireshark trace on PC

2c. Start the printer writer on AS/400

2d. Perform the capture

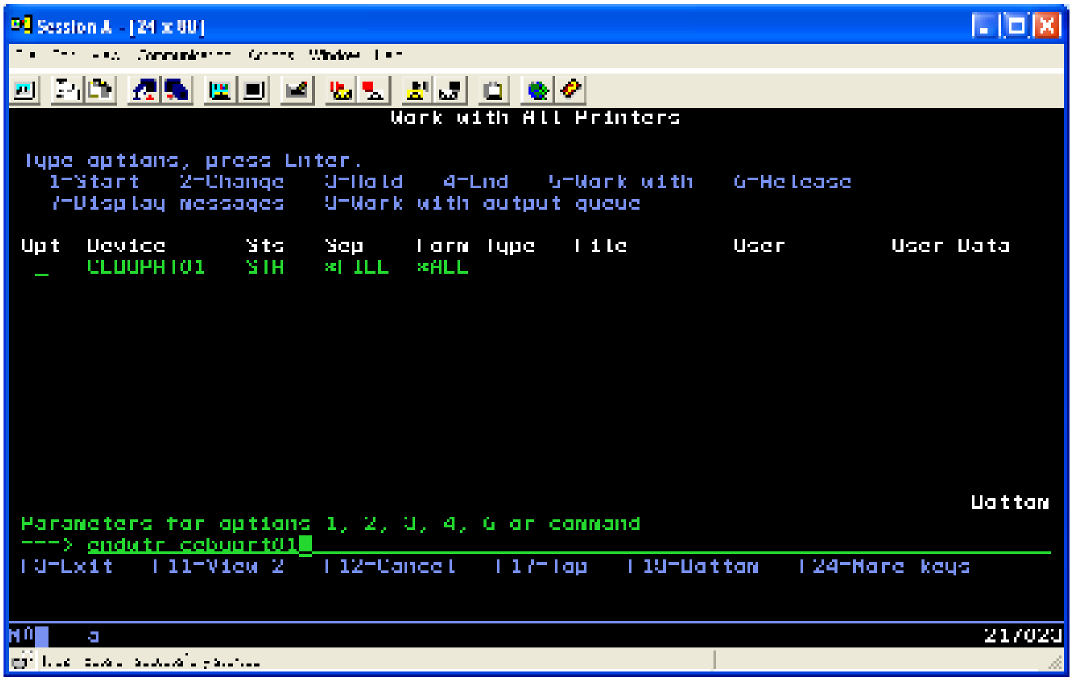
These sub-steps are detailed below.

2a. Stop the writer on the AS/400

This step is necessary to ensure that we get a good trace that captures the beginning of the job until the end. This part is normally performed by the customer's AS/400 system operator.

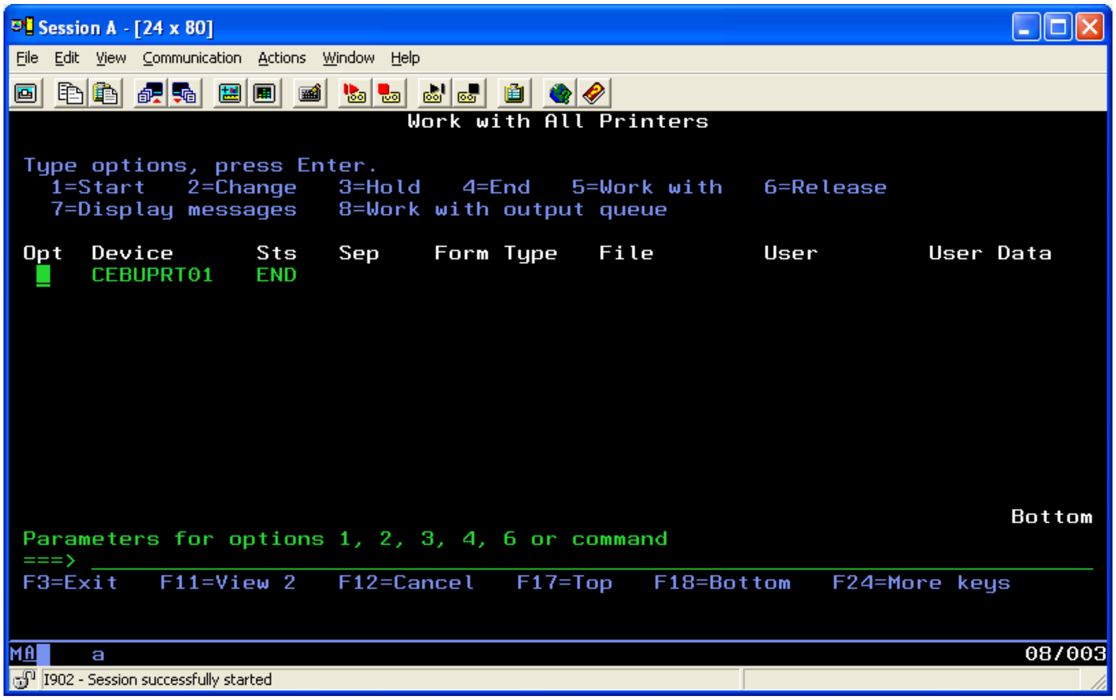
1. Log on to the AS/400.

2. End the print writer to be used by typing `ENDWTR name_of_writer`.



```
                              Work with All Printers

 Type options, press Enter.
   1=Start   2=Change   3=Hold   4=End   5=Work with   6=Release
   7=Display messages   8=Work with output queue

 Opt  Device       Sts    Sep     Form Type   File         User         User Data
  _   CEBUPRT01    STR    *FILE   *ALL

                                                                          Bottom
 Parameters for options 1, 2, 3, 4, 6 or command
 ===> endwtr cebuprt01
 F3=Exit   F11=View 2   F12=Cancel   F17=Top   F18=Bottom   F24=More keys
```

3. Wait or refresh until the writer status is END.



```
                             Work with All Printers

 Type options, press Enter.
   1=Start   2=Change    3=Hold    4=End    5=Work with    6=Release
   7=Display messages    8=Work with output queue

 Opt  Device       Sts    Sep    Form Type   File        User        User Data
      CEBUPRT01    END




                                                                         Bottom
 Parameters for options 1, 2, 3, 4, 6 or command
 ===>
 F3=Exit   F11=View 2   F12=Cancel   F17=Top   F18=Bottom   F24=More keys

MA     a                                                                08/003
I902 - Session successfully started
```

4. Proceed to step 2B.

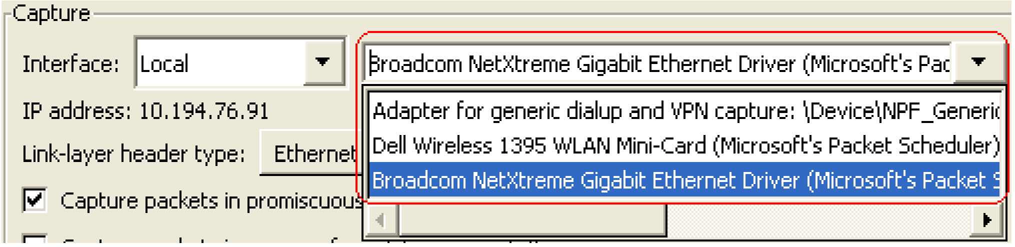
2B. Start the Wireshark trace on the PC

1. On a laptop or PC attached to hub, launch Wireshark application.

2. Select **Capture** menu and then **Options** to launch the Capture Options dialog.

3. Make the following changes in the **Capture Options** dialog

   a. Set **Interface** to “Local” then select Ethernet as the port to monitor.



Capture

Interface: Local | Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Pac

Adapter for generic dialup and VPN capture: \Device\NPF_Generic

Dell Wireless 1395 WLAN Mini-Card (Microsoft's Packet Scheduler)

Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet S

IP address: 10.194.76.91

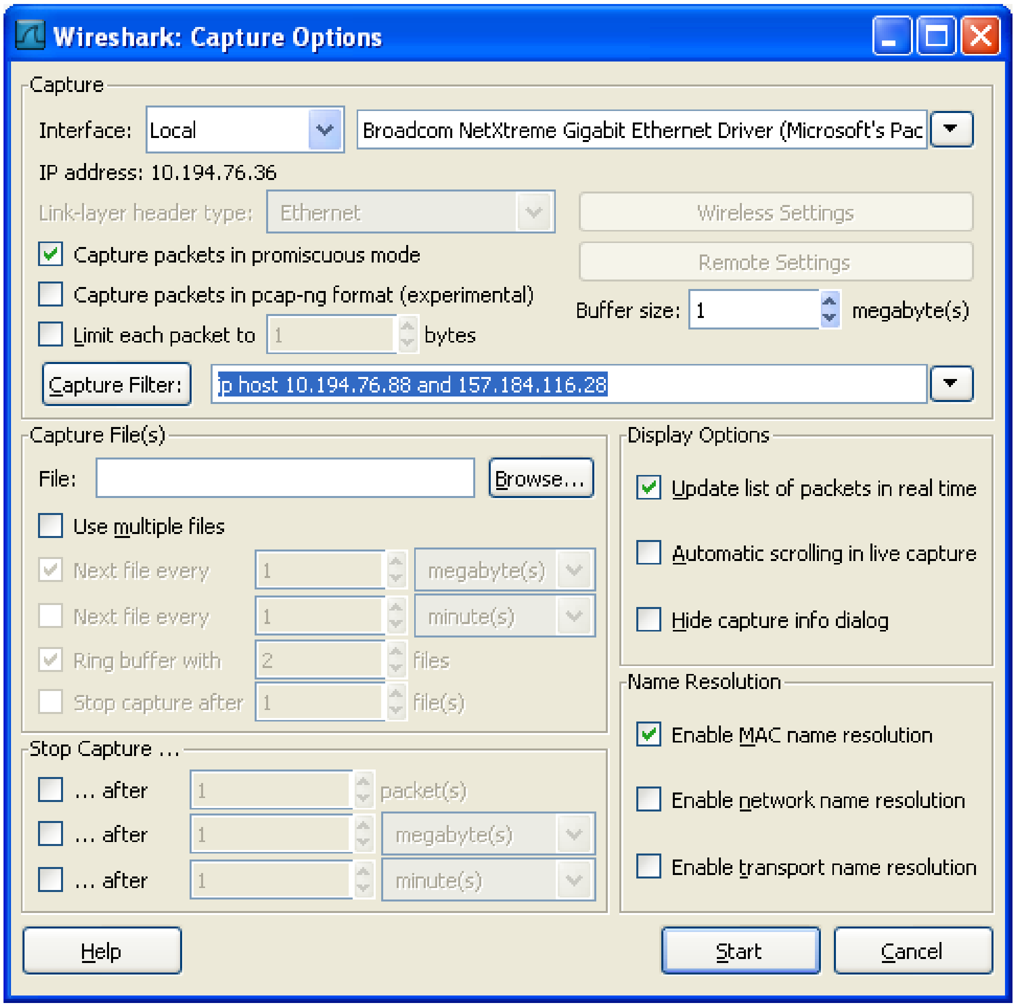
Link-layer header type: Ethernet

☑ Capture packets in promiscuous

   b. Check "Capture packet in promiscuous mode"

   c. In **Capture Filter**, specify the following filter string: `ip host  xxx.xxx.xxx.xx and xxx.xxx.xxx.xx`, where the first IP address refers to the server and the last IP address is for the printer.

4. The Options dialog should look something like this:



Wireshark: Capture Options

Capture

Interface: Local — Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Pac

IP address: 10.194.76.36

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

☐ Capture packets in pcap-ng format (experimental)

☐ Limit each packet to 1 bytes

Buffer size: 1 megabyte(s)

Capture Filter: ip host 10.194.76.88 and 157.184.116.28

Capture File(s)

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☑ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☐ Automatic scrolling in live capture

☐ Hide capture info dialog

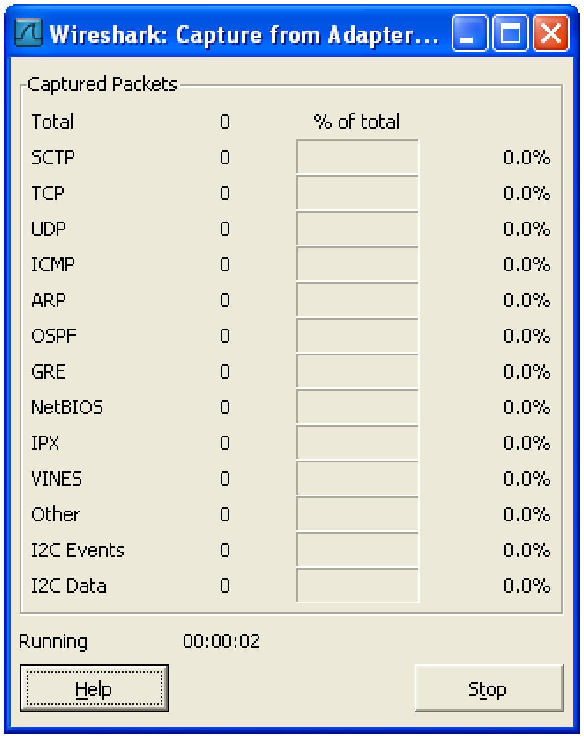
Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☐ Enable transport name resolution

5. Click **Start** to run the trace. The following capture dialog should launch:



Wireshark: Capture from Adapter...

Captured Packets

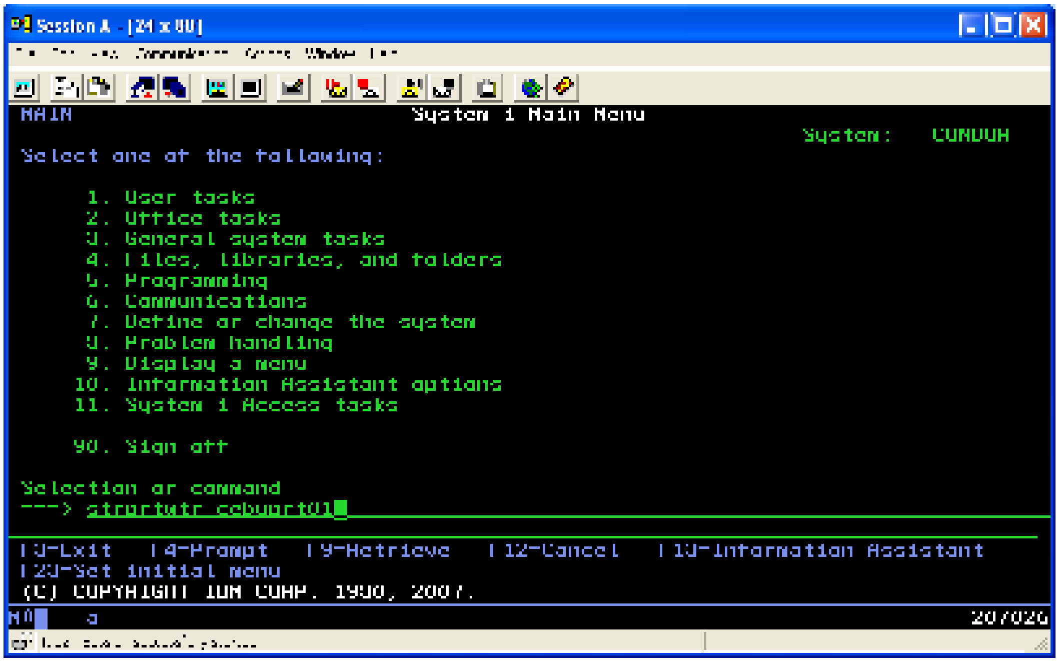
		% of total	
Total	0		
SCTP	0		0.0%
TCP	0		0.0%
UDP	0		0.0%
ICMP	0		0.0%
ARP	0		0.0%
OSPF	0		0.0%
GRE	0		0.0%
NetBIOS	0		0.0%
IPX	0		0.0%
VINES	0		0.0%
Other	0		0.0%
I2C Events	0		0.0%
I2C Data	0		0.0%

Running 00:00:02

6. Proceed to step 2c.

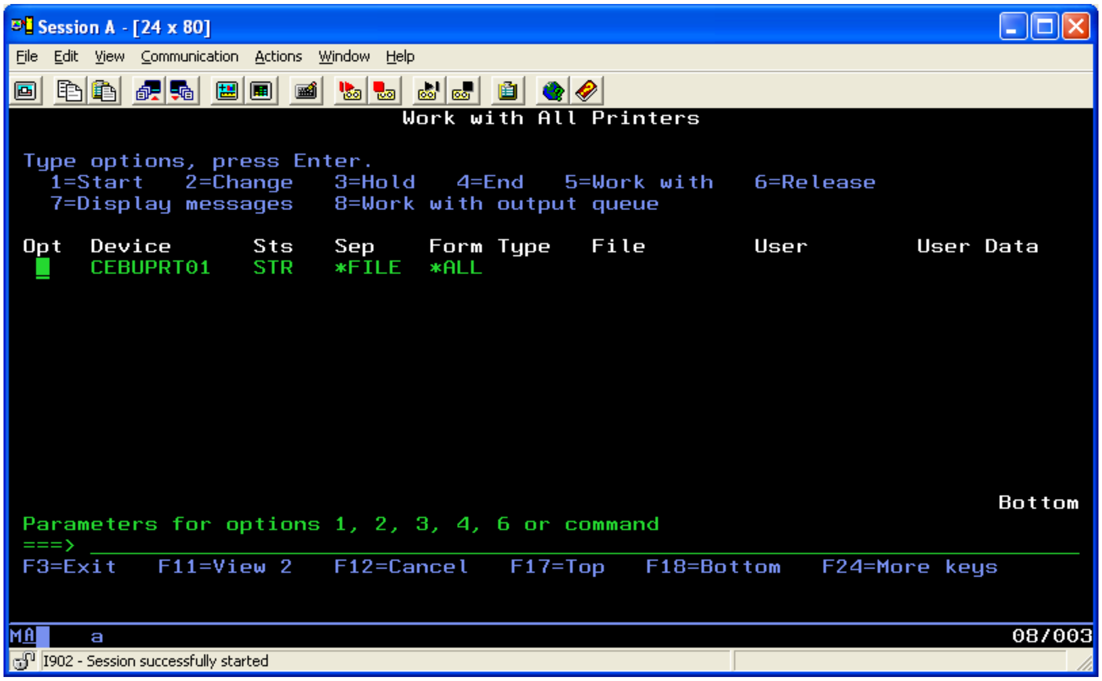
2c. Start the Writer on the AS/400

1. On the AS/400, start the writer by typing **STRPRTWTR name_of_writer**.



```
MAIN                           System i Main Menu
                                                             System:   CONDOR
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. System i Access tasks

    90. Sign off

Selection or command
===> strprtwtr cebuprt01

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2007.
MA     a                                                                 20/026
```

2. Wait (and refresh) until the writer status is **STR**.



```
                           Work with All Printers

Type options, press Enter.
  1=Start   2=Change   3=Hold   4=End   5=Work with   6=Release
  7=Display messages   8=Work with output queue

Opt  Device      Sts  Sep    Form Type    File         User         User Data
     CEBUPRT01   STR  *FILE  *ALL





                                                                         Bottom
Parameters for options 1, 2, 3, 4, 6 or command
===>
F3=Exit   F11=View 2   F12=Cancel   F17=Top   F18=Bottom   F24=More keys

MA     a                                                                 08/003
I902 - Session successfully started
```

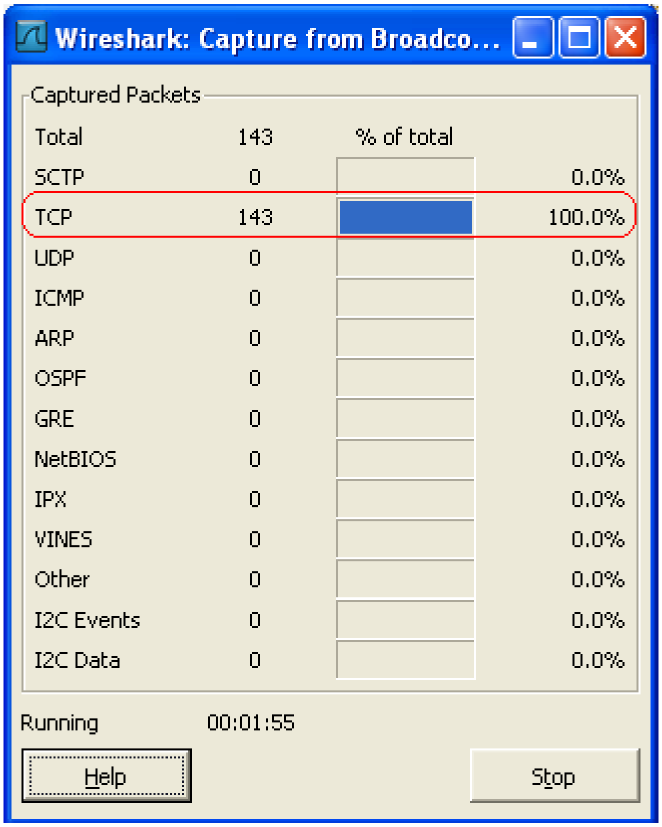
3. Proceed to step 2D.

2D. Perform the Print Job/Test to Capture On AS/400

1. Send the job to the printer.

2. Check the printer to see if job has started printing.

3. Monitor the Wireshark Capture Dialog to make sure that TCP packets are being captured



Captured Packets

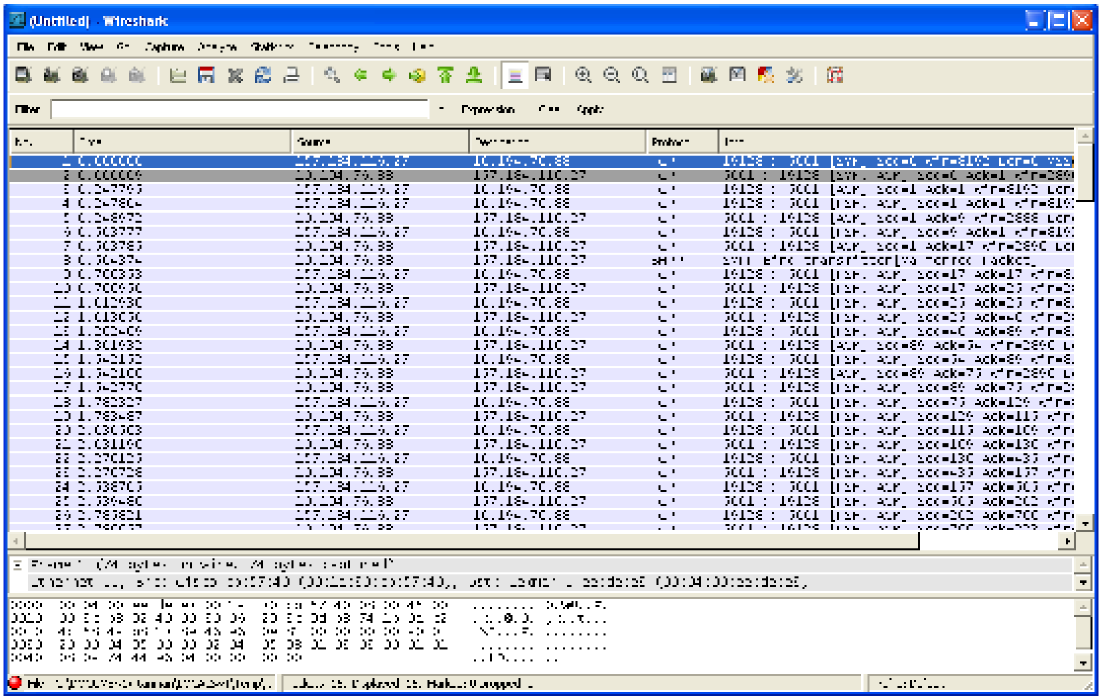
Total	143	% of total
SCTP	0	0.0%
TCP	143	100.0%
UDP	0	0.0%
ICMP	0	0.0%
ARP	0	0.0%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	0	0.0%
I2C Events	0	0.0%
I2C Data	0	0.0%

Running 00:01:55

4. Make sure job has completed printing.

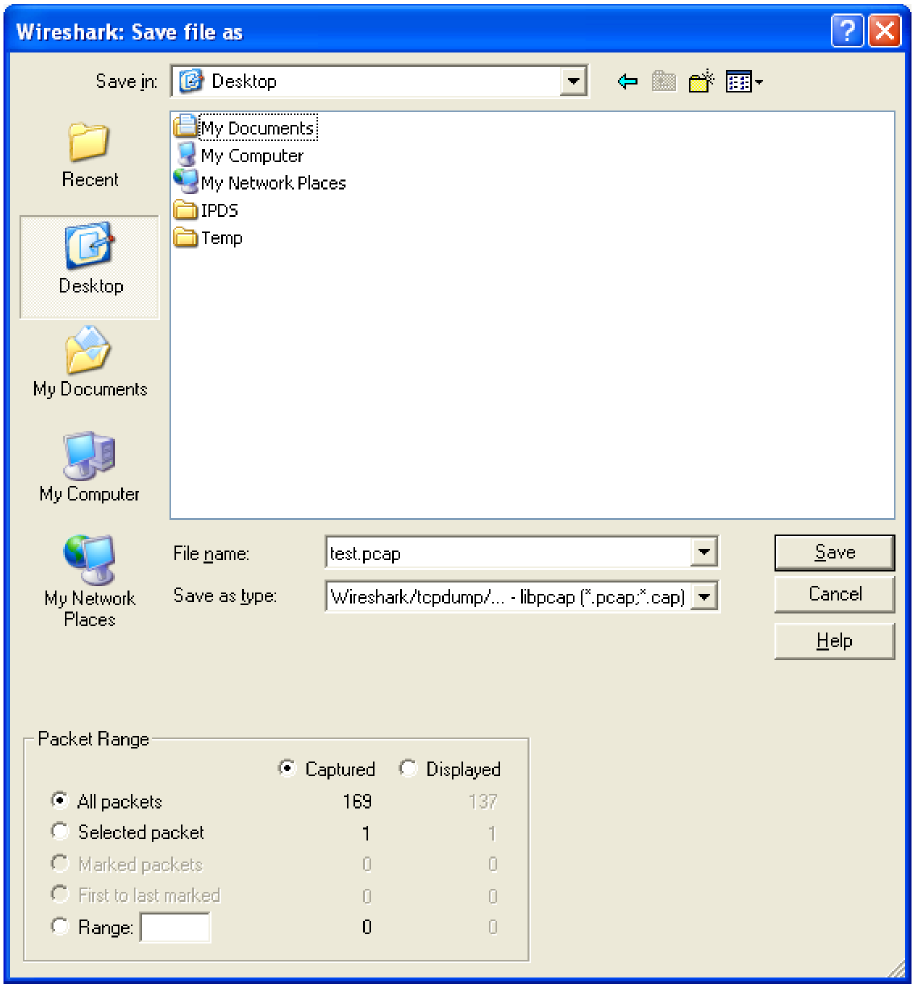
5. After job has completed printing, click **Stop** on the Wireshark Capture dialog.

6. The Wireshark application should now display the captured packets:



7. Click on File menu and then Save As to launch save dialog.

8. Save the file as a Wireshark tcpdump (*.pcap or *.cap).



Save in: Desktop

My Documents
My Computer
My Network Places
IPDS
Temp

File name: test.pcap

Save as type: Wireshark/tcpdump/... - libpcap (*.pcap;*.cap)

Packet Range

	● Captured	○ Displayed
● All packets	169	137
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0

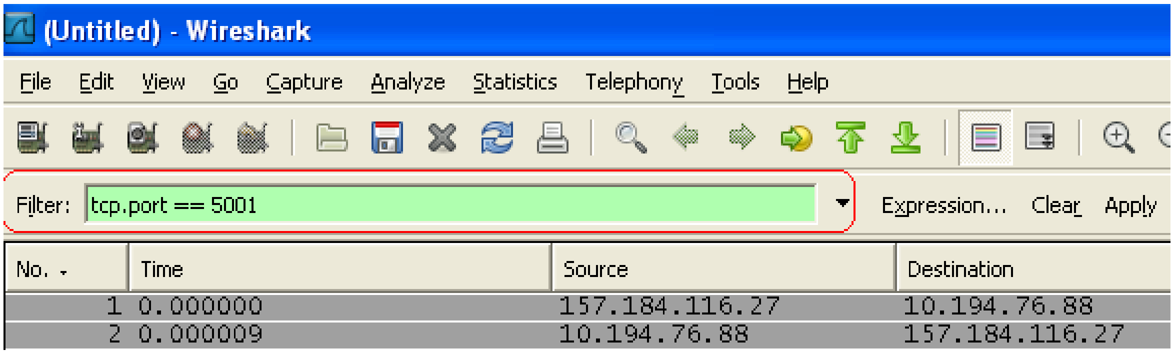
9. Once saved, proceed to step 3 to verify if you have a good trace.

STEP 3: VERIFY IF YOU HAVE THE CORRECT TRACE

A successful capture does not always indicate that the correct records have been captured. Thus, verification is necessary.

1. Open trace in Wireshark.

2. Under Filter, input `tcp.port == 5001`, where 5001 is the port used for IPDS. Use 9100 for non-IPDS jobs. .

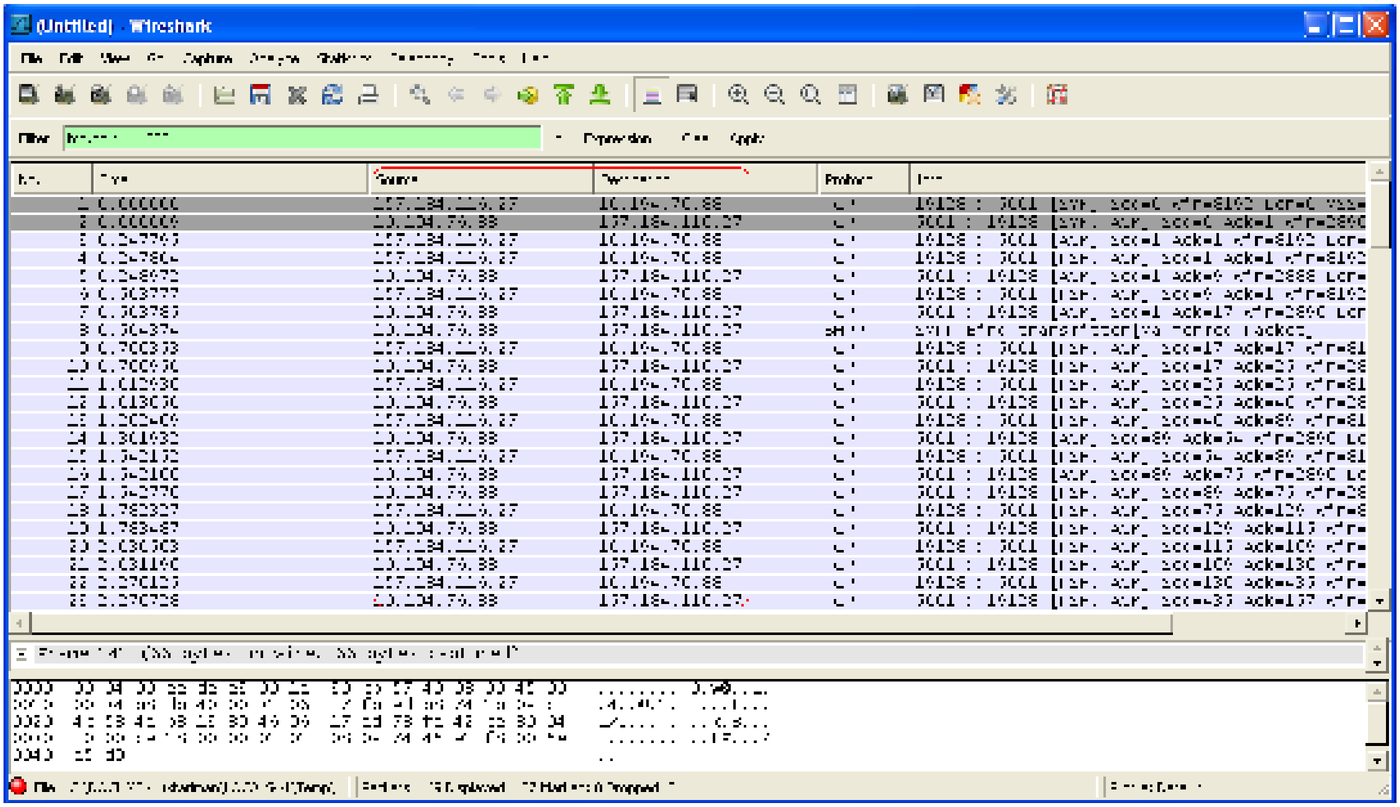


Filter: tcp.port == 5001

No.	Time	Source	Destination
1	0.000000	157.184.116.27	10.194.76.88
2	0.000009	10.194.76.88	157.184.116.27

3. Click **Apply**.

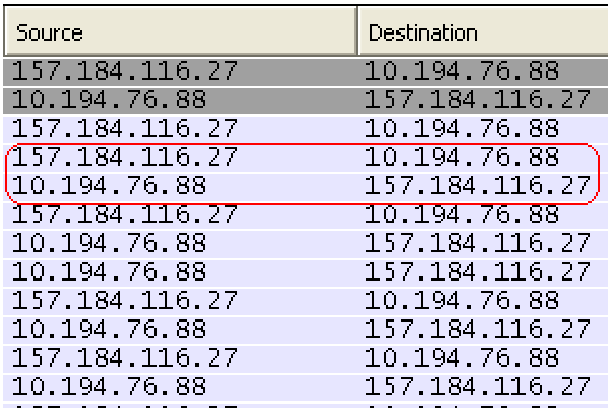
4. Verify that there are packets recorded for port 5001 (or 9100 and 9600 for non-IPDS).



```
No. Time      Source          Destination     Protocol Info
  1 0.000000  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [SYN] Seq=0 Win=8192 Len=0 MSS=
  2 0.000009  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [SYN, ACK] Seq=0 Ack=1 Win=2896
  3 0.247793  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [ACK] Seq=1 Ack=1 Win=8192 Len=
  4 0.247864  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=1 Ack=1 Win=8192
  5 0.248972  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [ACK] Seq=1 Ack=9 Win=2888 Len=
  6 0.303777  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=9 Ack=1 Win=8192
  7 0.303783  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [ACK] Seq=1 Ack=17 Win=2896 Len
  8 0.304374  10.194.76.88    157.184.116.27  [illegible]
  9 0.700373  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=17 Ack=17 Win=81
 10 0.700970  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [PSH, ACK] Seq=17 Ack=23 Win=28
 11 1.012930  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=23 Ack=23 Win=81
 12 1.013030  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [PSH, ACK] Seq=23 Ack=40 Win=28
 13 1.202409  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=40 Ack=89 Win=81
 14 1.301932  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [ACK] Seq=89 Ack=54 Win=2896 Le
 15 1.342132  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=54 Ack=89 Win=81
 16 1.342100  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [ACK] Seq=89 Ack=73 Win=2896 Le
 17 1.342770  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [PSH, ACK] Seq=89 Ack=73 Win=28
 18 1.782327  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=73 Ack=129 Win=8
 19 1.783487  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [PSH, ACK] Seq=129 Ack=113 Win=
 20 2.030303  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=113 Ack=109 Win=
 21 2.031190  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [PSH, ACK] Seq=109 Ack=130 Win=
 22 2.270123  157.184.116.27  10.194.76.88    TCP  19128 > 5001 [PSH, ACK] Seq=130 Ack=433 Win=
 23 2.270728  10.194.76.88    157.184.116.27  TCP  5001 > 19128 [PSH, ACK] Seq=433 Ack=137 Win=
```

5. If packets are available, check the packet Source and Destination to make sure that the IP addresses that appear are from the AS/400 and the printer.

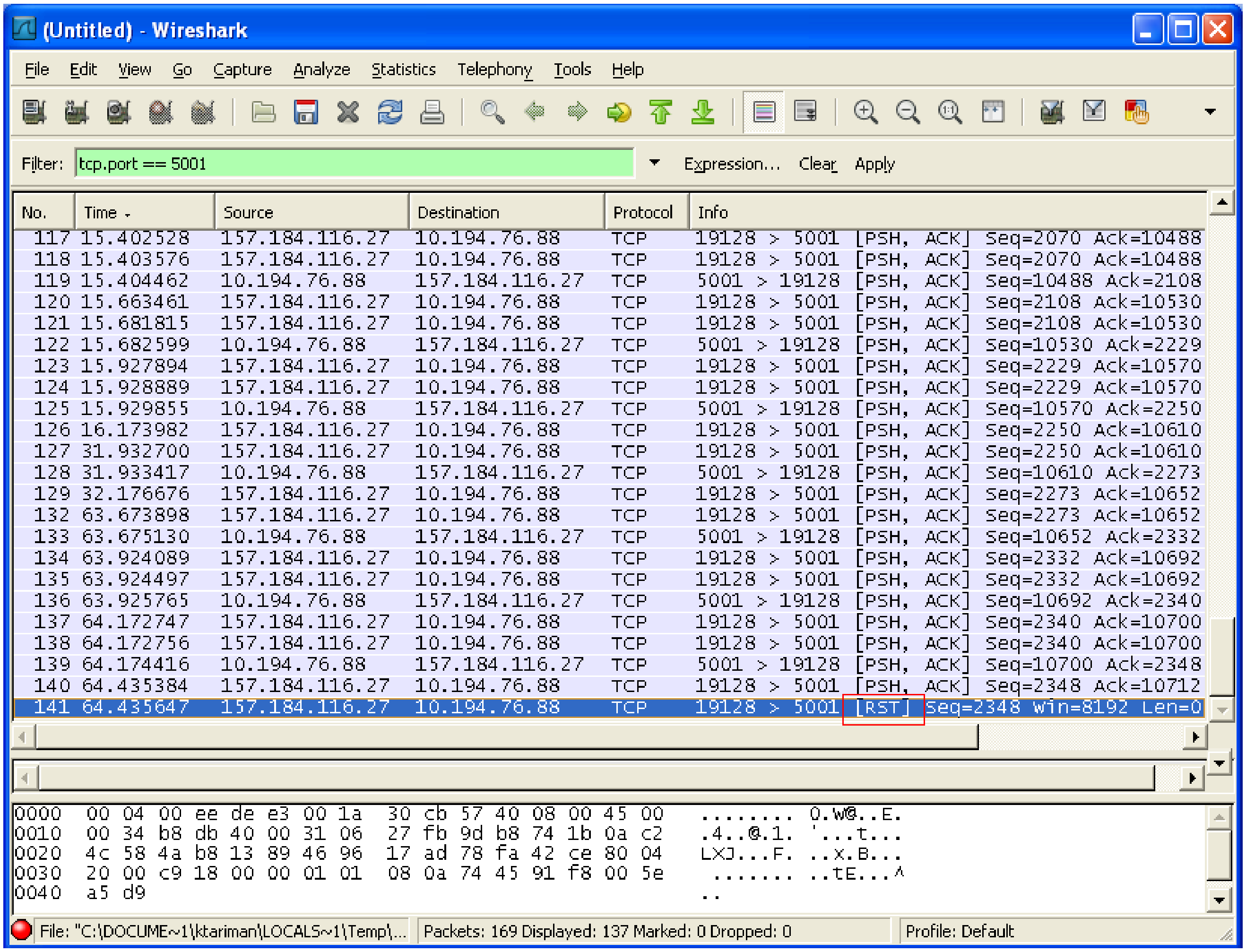
   For example, if the AS/400 IP is 157.184.116.27 and printer IP is 10.194.76.88, then the packets captured should show Source and Destination info like this (for bi-directional communication between server and printer):



Source	Destination
157.184.116.27	10.194.76.88
10.194.76.88	157.184.116.27
157.184.116.27	10.194.76.88
157.184.116.27	10.194.76.88
10.194.76.88	157.184.116.27
157.184.116.27	10.194.76.88
10.194.76.88	157.184.116.27
10.194.76.88	157.184.116.27
157.184.116.27	10.194.76.88
10.194.76.88	157.184.116.27
157.184.116.27	10.194.76.88
10.194.76.88	157.184.116.27

   If you do not see the IP address of the AS/400, check to see if you can ping the IP address from the laptop or PC. If not, then you may be tracking the wrong IP address for the host. Check with customer's network admin.

6. Scroll to the end of the trace and see if the last packet is a FIN or RST, which signifies that job has completed.



(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: tcp.port == 5001

```
No.  Time      Source          Destination     Protocol Info
117 15.402528 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2070 Ack=10488
118 15.403576 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2070 Ack=10488
119 15.404462 10.194.76.88   157.184.116.27 TCP  5001 > 19128 [PSH, ACK] Seq=10488 Ack=2108
120 15.663461 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2108 Ack=10530
121 15.681815 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2108 Ack=10530
122 15.682599 10.194.76.88   157.184.116.27 TCP  5001 > 19128 [PSH, ACK] Seq=10530 Ack=2229
123 15.927894 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2229 Ack=10570
124 15.928889 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2229 Ack=10570
125 15.929855 10.194.76.88   157.184.116.27 TCP  5001 > 19128 [PSH, ACK] Seq=10570 Ack=2250
126 16.173982 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2250 Ack=10610
127 31.932700 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2250 Ack=10610
128 31.933417 10.194.76.88   157.184.116.27 TCP  5001 > 19128 [PSH, ACK] Seq=10610 Ack=2273
129 32.176676 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2273 Ack=10652
132 63.673898 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2273 Ack=10652
133 63.675130 10.194.76.88   157.184.116.27 TCP  5001 > 19128 [PSH, ACK] Seq=10652 Ack=2332
134 63.924089 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2332 Ack=10692
135 63.924497 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2332 Ack=10692
136 63.925765 10.194.76.88   157.184.116.27 TCP  5001 > 19128 [PSH, ACK] Seq=10692 Ack=2340
137 64.172747 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2340 Ack=10700
138 64.172756 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2340 Ack=10700
139 64.174416 10.194.76.88   157.184.116.27 TCP  5001 > 19128 [PSH, ACK] Seq=10700 Ack=2348
140 64.435384 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [PSH, ACK] Seq=2348 Ack=10712
141 64.435647 157.184.116.27 10.194.76.88   TCP  19128 > 5001 [RST] Seq=2348 Win=8192 Len=0
```

```
0000  00 04 00 ee de e3 00 1a  30 cb 57 40 08 00 45 00   ........ 0.W@..E.
0010  00 34 b8 db 40 00 31 06  27 fb 9d b8 74 1b 0a c2   .4..@.1. '...t...
0020  4c 58 4a b8 13 89 46 96  17 ad 78 fa 42 ce 80 04   LXJ...F. ..x.B...
0030  20 00 c9 18 00 00 01 01  08 0a 74 45 91 f8 00 5e    ....... ..tE...^
0040  a5 d9                                              ..
```

File: "C:\DOCUME~1\ktariman\LOCALS~1\Temp\... Packets: 169 Displayed: 137 Marked: 0 Dropped: 0 Profile: Default

7. Lastly, if any of the verification steps fail, see section below.

Step 4: Send trace to PE

Send the trace file to TSC Level 3 who in turn sends it to PE. Please send the trace with the following information:

1. Description of job that was performed when trace A was captured.
2. Result of job that was performed when trace A was captured.
3. Printer that AS/400 was printing to when trace A was captured.

Good Example:

> "Trace1.pcap is the trace captured from a 20-page job sent to T654 that printed with missing bar code on page 3. Trace2.pcap is the trace captured from the same job sent to T644 that printed correctly."

Better Example:

> "Captured the following traces of a 20-page job first sent to T654 and then to T644:
> T654_missing_barcode_pg3.pcap and T644_OK_barcode.pcap"

Both examples are good and acceptable. However, the second example is better since the filenames are descriptive enough to be easily understandable and unambiguous. That is, we know exactly which file is which after downloading from database or email.

Can't get a Good Trace?

If you've performed the steps correctly but still fail verification (Step 3), repeat Steps 1 and 2 to see if there are items that you missed. Common items include:

- Use of network switch instead of hub
- Use of incorrect IP address
- Starting the trace after the job has printed
- Stopping the trace too early (while job is still printing)
- Customer's network topology uses multiple switches and routers and is different from diagram in document.

If you are not able to capture the trace, please report the problem to PE with the following info:

1. Sample of trace that was captured so we can cross-verify.
2. Description of what job was performed when trace in #1 was captured.
3. Diagram or description of setup used during network trace capture
4. Description of problems encountered during network trace capture.
5. Description of any limitations or restrictions in customer's current network setup, e.g. Customer does not want to detach printer from network, etc.

IMPORTANT: If security restrictions exist for the network, then it may not be possible to capture a good Wireshark trace at all. Please contact your PE for alternatives. There are other ways for gathering information about the customer's job, such as exporting of spool files into SAVF, capturing a USB trace, or capturing a debug trace.