07/26/2010

RICOH

Technical Information:

Extracting a Print Capture From a Network Packet Capture Using Wireshark White Paper

Document Version 1.0

Notice:

THIS DOCUMENT MAY NOT BE REPRODUCED OR DISTRIBUTED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH COMPANY LIMITED. RICOH COMPANY LIMITED RETAINS THE SOLE DISCRETION TO GRANT OR DENY CONSENT TO ANY PERSON OR PARTY.

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

The content of this document, and the appearance, features and specifications of Ricoh products are subject to change from time to time without notice. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty. Ricoh does not provide legal, accounting or auditing advice, or represent or warrant that our products or services will ensure that you are in compliance with any law. Customer is responsible for making the final selection of solution and technical architectures, and for ensuring its own compliance with various laws such as the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA).

Version History:

Version	Issue Date	Revised item
1.0	Apr. 6, 2007	1st Release

NOTE:

Throughout this document you may see references such as 04A (2004 Autumn) or 05S (2005 Spring). You will only see an A (Autumn) or S (Spring) attached to the last two digits of a year.

These two seasons reflect the time period the machines were manufactured.

INDEX

1. Introduction

This document describes how to extract a print capture from a network packet capture.

NOTE: *A print capture can be extracted from any unencrypted print data stream sent over the network. However, this document focuses on obtaining print captures of jobs sent using* ***DIPRINT (port 9100)*** *and* ***LPR****.*

2. Target Readers

This document is intended for the support staff of Ricoh family group companies and their subsidiaries.

3. Requirements

- The data should be unencrypted. If data is submitted to the printer using ssl, it will not be readable to the capturing PC.
- The data should be fully captured. In situations where session timeouts occur or the network is unstable, data might not be fully captured by the PC. Such a capture is not useful for extracting print data from.
- All packet capturing tools should have a way to assemble captured packets into data. In this document we will use Wireshark (formerly Ethereal). For details, please visit: http://www.wireshark.org/

4. Procedure

a. Download and install Wireshark on a PC.

b. Capture print job(s) as network packets and save them as a file:
The entire packet capture should be saved as a file before extracting print captures from it.

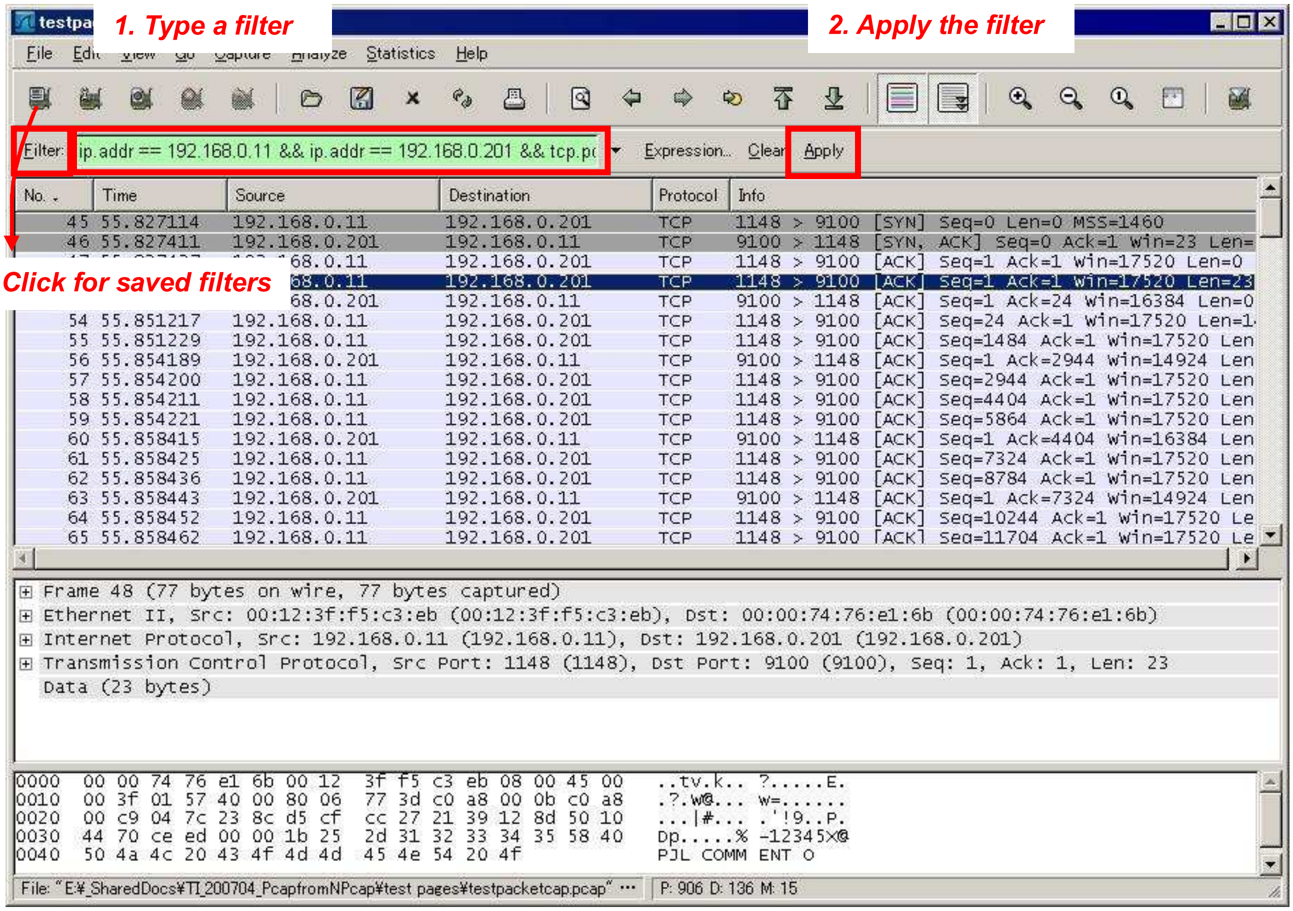
c. Filter the Packets:
Filter the packets by the IP addresses of the sender, the destination and the port number. ***(Figure 3a)***

NOTE: *These are 2 examples that are useful for our purposes in this document. You might want to experiment with your own filters.*

- **LPR** printing:
ip.addr == xxx.xxx.xxx.xxx && ip.addr == xxx.xxx.xxx.xxx && tcp.port == 515
- **DIPRINT** (port 9100 printing):
ip.addr == xxx.xxx.xxx.xxx && ip.addr == xxx.xxx.xxx.xxx && tcp.port == 9100

In the below example, the sender has an IP address of 192.168.0.11 and the printer has an IP address of 192.168.0.201. Packets are filtered by both IP addresses and TCP port 9100.

Figure 3a - Filtering the Packets



Filter: ip.addr == 192.168.0.11 && ip.addr == 192.168.0.201 && tcp.pc

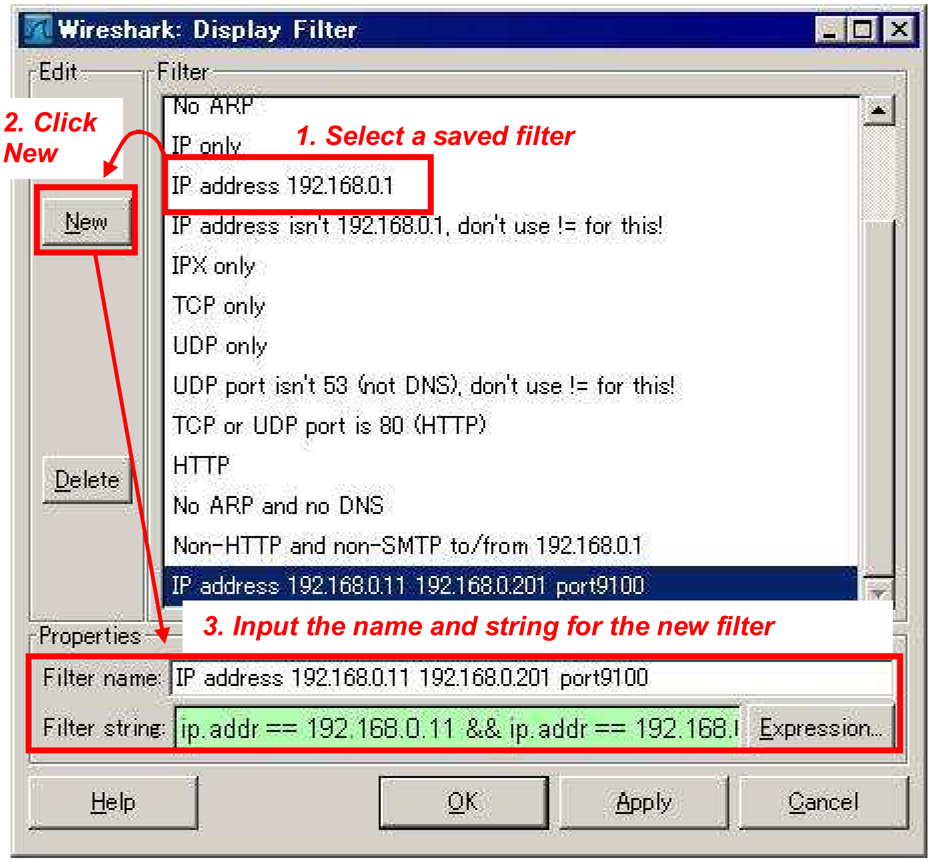
```
No. -  Time        Source          Destination     Protocol  Info
    45 55.827114   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [SYN] Seq=0 Len=0 MSS=1460
    46 55.827411   192.168.0.201   192.168.0.11    TCP       9100 > 1148 [SYN, ACK] Seq=0 Ack=1 Win=23 Len=
                     68.0.11       192.168.0.201   TCP       1148 > 9100 [ACK] Seq=1 Ack=1 Win=17520 Len=0
                     68.0.11       192.168.0.201   TCP       1148 > 9100 [ACK] Seq=1 Ack=1 Win=17520 Len=23
                     68.0.201      192.168.0.11    TCP       9100 > 1148 [ACK] Seq=1 Ack=24 Win=16384 Len=0
    54 55.851217   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=24 Ack=1 Win=17520 Len=1
    55 55.851229   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=1484 Ack=1 Win=17520 Len
    56 55.854189   192.168.0.201   192.168.0.11    TCP       9100 > 1148 [ACK] Seq=1 Ack=2944 Win=14924 Len
    57 55.854200   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=2944 Ack=1 Win=17520 Len
    58 55.854211   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=4404 Ack=1 Win=17520 Len
    59 55.854221   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=5864 Ack=1 Win=17520 Len
    60 55.858415   192.168.0.201   192.168.0.11    TCP       9100 > 1148 [ACK] Seq=1 Ack=4404 Win=16384 Len
    61 55.858425   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=7324 Ack=1 Win=17520 Len
    62 55.858436   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=8784 Ack=1 Win=17520 Len
    63 55.858443   192.168.0.201   192.168.0.11    TCP       9100 > 1148 [ACK] Seq=1 Ack=7324 Win=14924 Len
    64 55.858452   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=10244 Ack=1 Win=17520 Le
    65 55.858462   192.168.0.11    192.168.0.201   TCP       1148 > 9100 [ACK] Seq=11704 Ack=1 Win=17520 Le
```

```
⊞ Frame 48 (77 bytes on wire, 77 bytes captured)
⊞ Ethernet II, Src: 00:12:3f:f5:c3:eb (00:12:3f:f5:c3:eb), Dst: 00:00:74:76:e1:6b (00:00:74:76:e1:6b)
⊞ Internet Protocol, Src: 192.168.0.11 (192.168.0.11), Dst: 192.168.0.201 (192.168.0.201)
⊞ Transmission Control Protocol, Src Port: 1148 (1148), Dst Port: 9100 (9100), Seq: 1, Ack: 1, Len: 23
  Data (23 bytes)
```

```
0000  00 00 74 76 e1 6b 00 12  3f f5 c3 eb 08 00 45 00   ..tv.k.. ?.....E.
0010  00 3f 01 57 40 00 80 06  77 3d c0 a8 00 0b c0 a8   .?.W@... w=......
0020  00 c9 04 7c 23 8c d5 cf  cc 27 21 39 12 8d 50 10   ...|#... .'!9..P.
0030  44 70 ce ed 00 00 1b 25  2d 31 32 33 34 35 58 40   Dp.....% -12345X@
0040  50 4a 4c 20 43 4f 4d 4d  45 4e 54 20 4f            PJL COMM ENT O
```

File: "E:¥_SharedDocs¥TI_200704_PcapfromNPcap¥test pages¥testpacketcap.pcap" ··· | P: 906 D: 136 M: 15

Wireshark has a list of saved filters. Click the [Filter] button (See ***Figure 3a*** on previous page.) to view them or create a new one (***Figure 3b***).



1. Select a saved filter

2. Click New

3. Input the name and string for the new filter

No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
TCP or UDP port is 80 (HTTP)
HTTP
No ARP and no DNS
Non-HTTP and non-SMTP to/from 192.168.0.1
IP address 192.168.0.11 192.168.0.201 port9100

Filter name: IP address 192.168.0.11 192.168.0.201 port9100

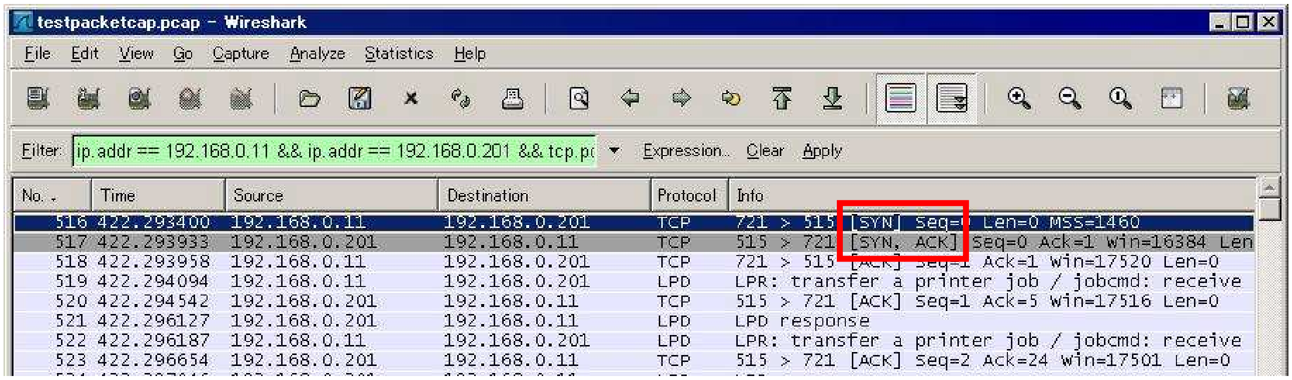
Filter string: ip.addr == 192.168.0.11 && ip.addr == 192.168.

Figure 3b - Creating a New Filter

d. Find a Particular TCP Session:

Sessions begin with a SYN flag and end with a FIN flag. ***(Figure 4a)***

Individual sessions can be isolated by filtering the sender port. ***(Figure 4b)***

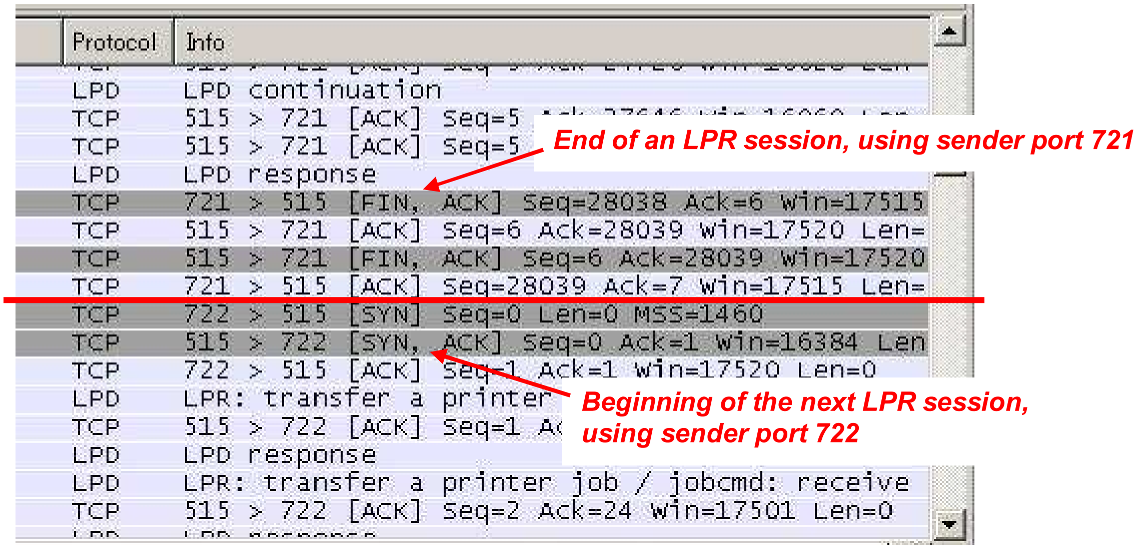


testpacketcap.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: ip.addr == 192.168.0.11 && ip.addr == 192.168.0.201 && tcp.pc

```
No. .  Time           Source          Destination     Protocol  Info
  516 422.293400  192.168.0.11    192.168.0.201   TCP       721 > 515 [SYN] Seq=0 Len=0 MSS=1460
  517 422.293933  192.168.0.201   192.168.0.11    TCP       515 > 721 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len
  518 422.293958  192.168.0.11    192.168.0.201   TCP       721 > 515 [ACK] Seq=1 Ack=1 Win=17520 Len=0
  519 422.294094  192.168.0.11    192.168.0.201   LPD       LPR: transfer a printer job / jobcmd: receive
  520 422.294542  192.168.0.201   192.168.0.11    TCP       515 > 721 [ACK] Seq=1 Ack=5 Win=17516 Len=0
  521 422.296127  192.168.0.201   192.168.0.11    LPD       LPD response
  522 422.296187  192.168.0.11    192.168.0.201   LPD       LPR: transfer a printer job / jobcmd: receive
  523 422.296654  192.168.0.201   192.168.0.11    TCP       515 > 721 [ACK] Seq=2 Ack=24 Win=17501 Len=0
```

Figure 4a - Session SYN/ACK flags



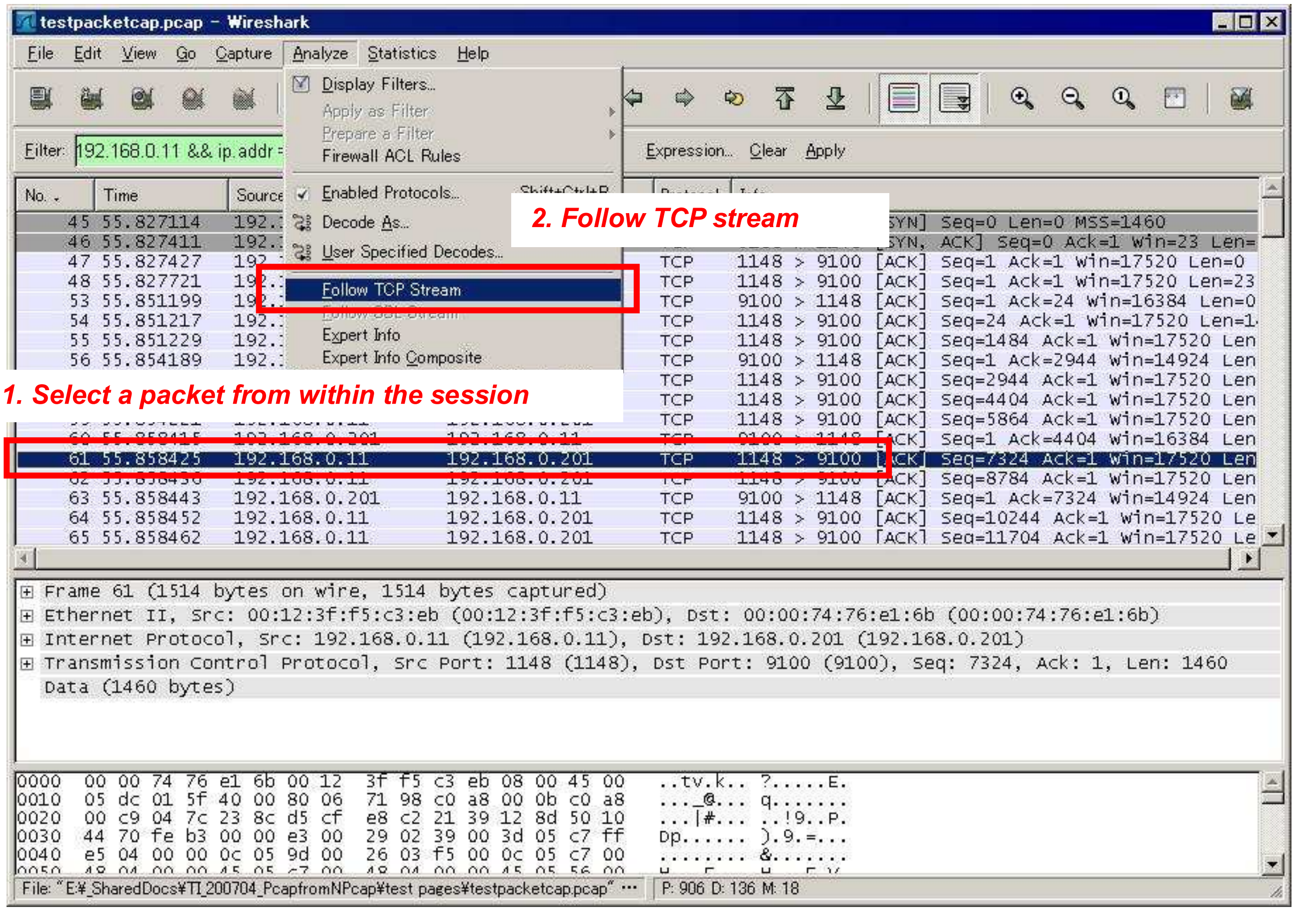
```
Protocol  Info
LPD       LPD continuation
TCP       515 > 721 [ACK] Seq=5
TCP       515 > 721 [ACK] Seq=5
LPD       LPD response
TCP       721 > 515 [FIN, ACK] Seq=28038 Ack=6 Win=17515
TCP       515 > 721 [ACK] Seq=6 Ack=28039 Win=17520 Len=
TCP       515 > 721 [FIN, ACK] Seq=6 Ack=28039 Win=17520
TCP       721 > 515 [ACK] Seq=28039 Ack=7 Win=17515 Len=
TCP       722 > 515 [SYN] Seq=0 Len=0 MSS=1460
TCP       515 > 722 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len
TCP       722 > 515 [ACK] Seq=1 Ack=1 Win=17520 Len=0
LPD       LPR: transfer a printer
TCP       515 > 722 [ACK] Seq=1 Ac
LPD       LPD response
LPD       LPR: transfer a printer job / jobcmd: receive
TCP       515 > 722 [ACK] Seq=2 Ack=24 Win=17501 Len=0
```

End of an LPR session, using sender port 721

Beginning of the next LPR session, using sender port 722

e. Extract the Packets from the Session Using “Follow TCP Stream”:

Select one of the TCP packets in the session. Click [Analyze] and select [Follow TCP Stream]. ***(Figure 5)***



Filter: 192.168.0.11 && ip.addr =

2. Follow TCP stream

1. Select a packet from within the session

```
45 55.827114   192.1                                            [SYN] Seq=0 Len=0 MSS=1460
46 55.827411   192.1                                            [SYN, ACK] Seq=0 Ack=1 Win=23 Len=
47 55.827427   192                                  TCP   1148 > 9100 [ACK] Seq=1 Ack=1 Win=17520 Len=0
48 55.827721   192.1                                TCP   1148 > 9100 [ACK] Seq=1 Ack=1 Win=17520 Len=23
53 55.851199   192.1                                TCP   9100 > 1148 [ACK] Seq=1 Ack=24 Win=16384 Len=0
54 55.851217   192.1                                TCP   1148 > 9100 [ACK] Seq=24 Ack=1 Win=17520 Len=1
55 55.851229   192.1                                TCP   1148 > 9100 [ACK] Seq=1484 Ack=1 Win=17520 Len
56 55.854189   192.1                                TCP   9100 > 1148 [ACK] Seq=1 Ack=2944 Win=14924 Len
                                                    TCP   1148 > 9100 [ACK] Seq=2944 Ack=1 Win=17520 Len
                                                    TCP   1148 > 9100 [ACK] Seq=4404 Ack=1 Win=17520 Len
59 55.854221   192.168.0.11     192.168.0.201       TCP   1148 > 9100 [ACK] Seq=5864 Ack=1 Win=17520 Len
60 55.858415   192.168.0.201    192.168.0.11        TCP   9100 > 1148 [ACK] Seq=1 Ack=4404 Win=16384 Len
61 55.858425   192.168.0.11     192.168.0.201       TCP   1148 > 9100 [ACK] Seq=7324 Ack=1 Win=17520 Len
62 55.858436   192.168.0.11     192.168.0.201       TCP   1148 > 9100 [ACK] Seq=8784 Ack=1 Win=17520 Len
63 55.858443   192.168.0.201    192.168.0.11        TCP   9100 > 1148 [ACK] Seq=1 Ack=7324 Win=14924 Len
64 55.858452   192.168.0.11     192.168.0.201       TCP   1148 > 9100 [ACK] Seq=10244 Ack=1 Win=17520 Le
65 55.858462   192.168.0.11     192.168.0.201       TCP   1148 > 9100 [ACK] Seq=11704 Ack=1 Win=17520 Le
```

```
⊞ Frame 61 (1514 bytes on wire, 1514 bytes captured)
⊞ Ethernet II, Src: 00:12:3f:f5:c3:eb (00:12:3f:f5:c3:eb), Dst: 00:00:74:76:e1:6b (00:00:74:76:e1:6b)
⊞ Internet Protocol, Src: 192.168.0.11 (192.168.0.11), Dst: 192.168.0.201 (192.168.0.201)
⊞ Transmission Control Protocol, Src Port: 1148 (1148), Dst Port: 9100 (9100), Seq: 7324, Ack: 1, Len: 1460
  Data (1460 bytes)
```

```
0000  00 00 74 76 e1 6b 00 12  3f f5 c3 eb 08 00 45 00   ..tv.k.. ?.....E.
0010  05 dc 01 5f 40 00 80 06  71 98 c0 a8 00 0b c0 a8   ..._@... q.......
0020  00 c9 04 7c 23 8c d5 cf  e8 c2 21 39 12 8d 50 10   ...|#... ..!9..P.
0030  44 70 fe b3 00 00 e3 00  29 02 39 00 3d 05 c7 ff   Dp...... ).9.=...
0040  e5 04 00 00 0c 05 9d 00  26 03 f5 00 0c 05 c7 00   ........ &.......
0050  48 04 00 00 45 05 c7 00  48 04 00 00 45 05 56 00   H...E... H...E.V.
```

File: “E:¥_SharedDocs¥TI_200704_PcapfromNPcap¥test pages¥testpacketcap.pcap” ··· P: 906 D: 136 M: 18

f. Save the Data as a Print Capture File:

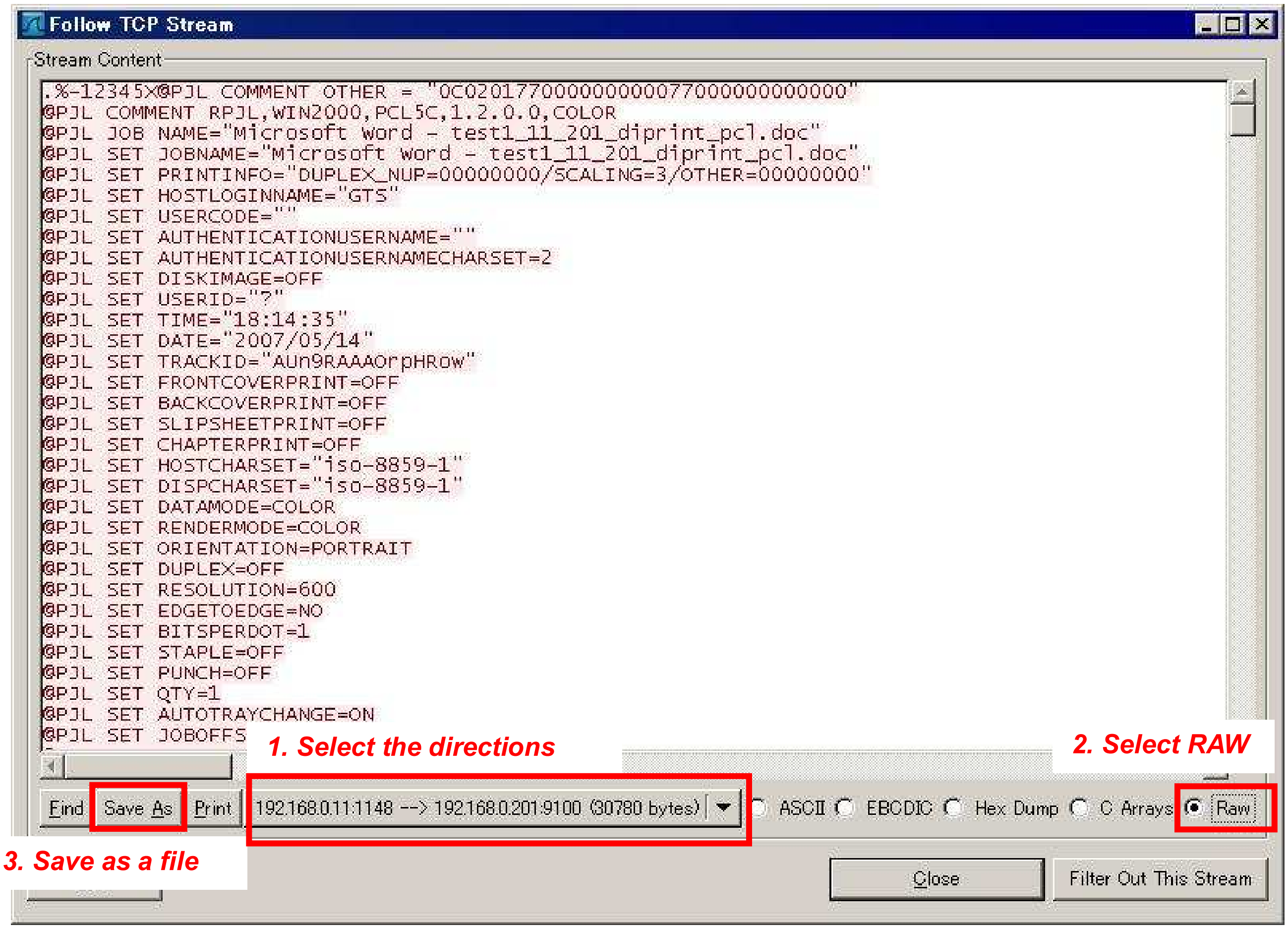
The following procedure will extract the captured data to a file ***(Figure 6)***:

1) Select the direction of the data stream (sender to destination).

   (This is necessary in order to exclude back-channel data from a receiver, such as USTATUS)

2) Select **RAW** for data type.

3) Click [Save As] to save the data as a file.



```
.%-12345X@PJL COMMENT OTHER = "0C020177000000000077000000000000"
@PJL COMMENT RPJL,WIN2000,PCL5C,1.2.0.0,COLOR
@PJL JOB NAME="Microsoft Word - test1_11_201_diprint_pcl.doc"
@PJL SET JOBNAME="Microsoft Word - test1_11_201_diprint_pcl.doc"
@PJL SET PRINTINFO="DUPLEX_NUP=00000000/SCALING=3/OTHER=00000000"
@PJL SET HOSTLOGINNAME="GTS"
@PJL SET USERCODE=""
@PJL SET AUTHENTICATIONUSERNAME=""
@PJL SET AUTHENTICATIONUSERNAMECHARSET=2
@PJL SET DISKIMAGE=OFF
@PJL SET USERID="?"
@PJL SET TIME="18:14:35"
@PJL SET DATE="2007/05/14"
@PJL SET TRACKID="AUn9RAAAOrpHRow"
@PJL SET FRONTCOVERPRINT=OFF
@PJL SET BACKCOVERPRINT=OFF
@PJL SET SLIPSHEETPRINT=OFF
@PJL SET CHAPTERPRINT=OFF
@PJL SET HOSTCHARSET="iso-8859-1"
@PJL SET DISPCHARSET="iso-8859-1"
@PJL SET DATAMODE=COLOR
@PJL SET RENDERMODE=COLOR
@PJL SET ORIENTATION=PORTRAIT
@PJL SET DUPLEX=OFF
@PJL SET RESOLUTION=600
@PJL SET EDGETOEDGE=NO
@PJL SET BITSPERDOT=1
@PJL SET STAPLE=OFF
@PJL SET PUNCH=OFF
@PJL SET QTY=1
@PJL SET AUTOTRAYCHANGE=ON
@PJL SET JOBOFFS
```

192.168.0.11:1148 --> 192.168.0.201:9100 (30780 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

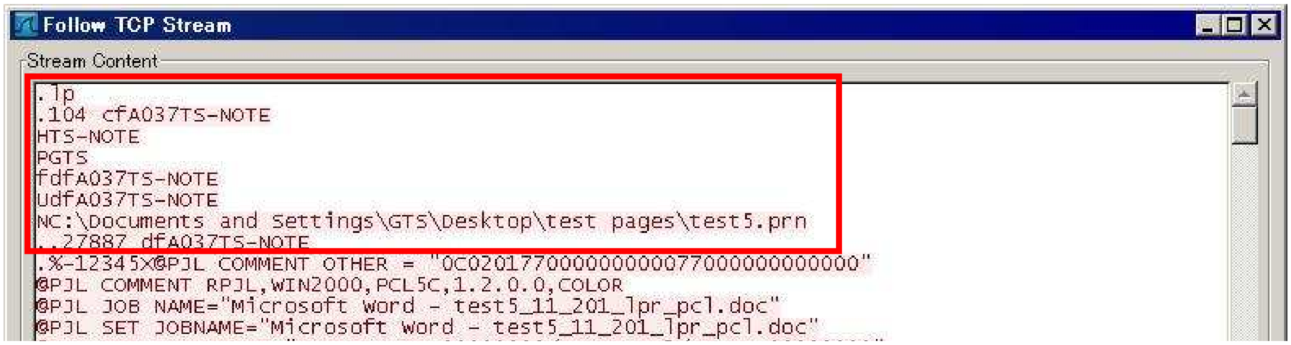
g. Remove LPR Data:
In the case of LPR, LPR data has to be removed from the file.

The LPR data can be sent before or after the print data:

- If the LPR data is sent before the print data, LPR data will appear at the beginning of the file. ***(Figure 7a)***
- If the LPR data is sent after the data, LPR data will appear at the beginning and at the end of the file. ***(Figure 7b)***

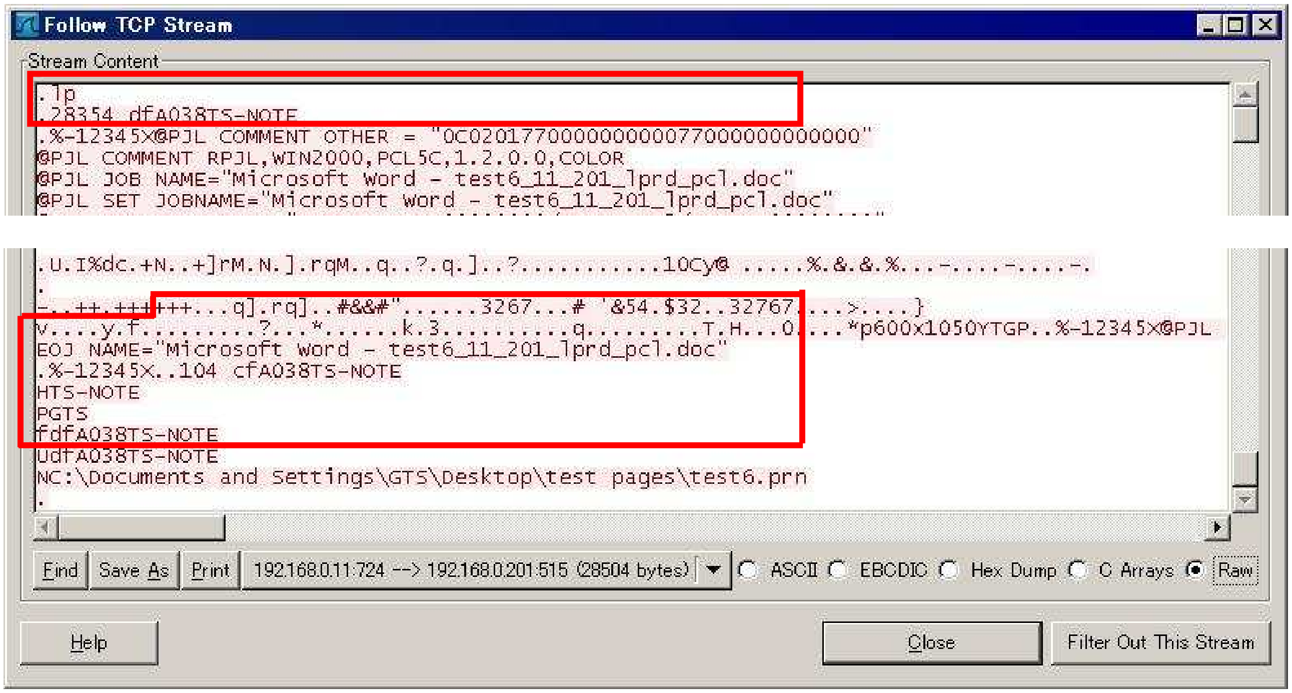
The following procedure will remove the LPR data:

1. Save the print capture file first.
2. Open the file with a binary editor and remove the LPR data. ***(Figure 7c** on next page**)***



```
.lp
.104 cfA037TS-NOTE
HTS-NOTE
PGTS
fdfA037TS-NOTE
UdfA037TS-NOTE
NC:\Documents and Settings\GTS\Desktop\test pages\test5.prn
..27887 dfA037TS-NOTE
.%-12345X@PJL COMMENT OTHER = "0C020177000000000077000000000000"
@PJL COMMENT RPJL,WIN2000,PCL5C,1.2.0.0,COLOR
@PJL JOB NAME="Microsoft Word - test5_11_201_lpr_pcl.doc"
@PJL SET JOBNAME="Microsoft Word - test5_11_201_lpr_pcl.doc"
```

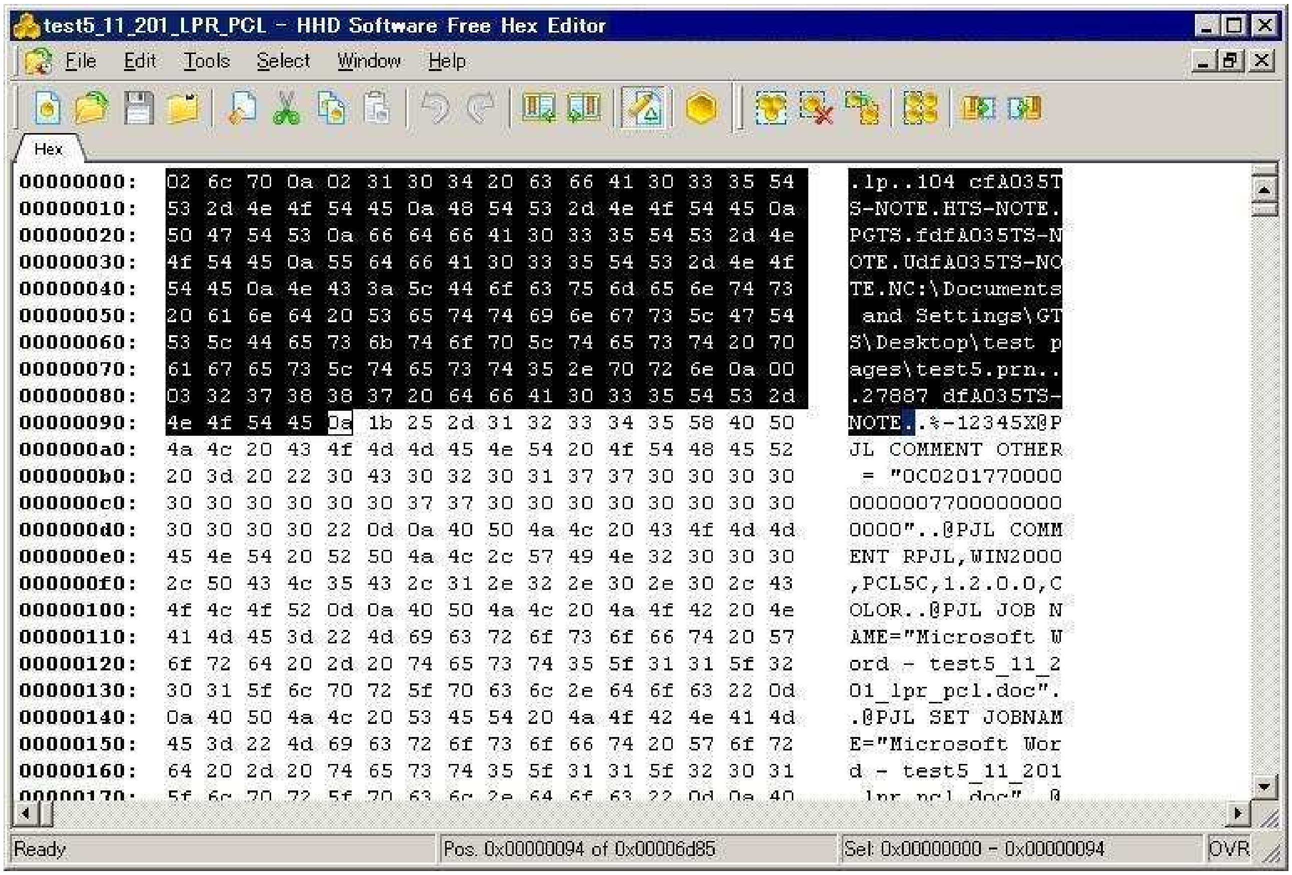
Figure 7a - LPR data at the beginning



```
.lp
.28354 dfA038TS-NOTE
.%-12345X@PJL COMMENT OTHER = "0C020177000000000077000000000000"
@PJL COMMENT RPJL,WIN2000,PCL5C,1.2.0.0,COLOR
@PJL JOB NAME="Microsoft Word - test6_11_201_lprd_pcl.doc"
@PJL SET JOBNAME="Microsoft Word - test6_11_201_lprd_pcl.doc"
```

```
.U.I%dc.+N..+]rM.N.].rqM..q..?.q.]..?...........10Cy@ .....%.&.&.%...-.....-.....-.
.
-..++.++++++...q].rq]..#&&#"......3267...# '&54.$32..32767.....>.....}
V....y.f.........?...*......k.3..........q.........T.H...0....*p600x1050YTGP..%-12345X@PJL
EOJ NAME="Microsoft Word - test6_11_201_lprd_pcl.doc"
.%-12345X..104 cfA038TS-NOTE
HTS-NOTE
PGTS
fdfA038TS-NOTE
UdfA038TS-NOTE
NC:\Documents and Settings\GTS\Desktop\test pages\test6.prn
.
```

Figure 7b - LPR data at the beginning and the end


test5_11_201_LPR_PCL - HHD Software Free Hex Editor
File
Edit
Tools
Select
Window
Help
Hex
Ready
Pos. 0x00000094 of 0x00006d85
Sel: 0x00000000 - 0x00000094
OVR

```
00000000:  02 6c 70 0a 02 31 30 34 20 63 66 41 30 33 35 54   .lp..104 cfA035T
00000010:  53 2d 4e 4f 54 45 0a 48 54 53 2d 4e 4f 54 45 0a   S-NOTE.HTS-NOTE.
00000020:  50 47 54 53 0a 66 64 66 41 30 33 35 54 53 2d 4e   PGTS.fdfA035TS-N
00000030:  4f 54 45 0a 55 64 66 41 30 33 35 54 53 2d 4e 4f   OTE.UdfA035TS-NO
00000040:  54 45 0a 4e 43 3a 5c 44 6f 63 75 6d 65 6e 74 73   TE.NC:\Documents
00000050:  20 61 6e 64 20 53 65 74 74 69 6e 67 73 5c 47 54    and Settings\GT
00000060:  53 5c 44 65 73 6b 74 6f 70 5c 74 65 73 74 20 70   S\Desktop\test p
00000070:  61 67 65 73 5c 74 65 73 74 35 2e 70 72 6e 0a 00   ages\test5.prn..
00000080:  03 32 37 38 38 37 20 64 66 41 30 33 35 54 53 2d   .27887 dfA035TS-
00000090:  4e 4f 54 45 0a 1b 25 2d 31 32 33 34 35 58 40 50   NOTE..%-12345X@P
000000a0:  4a 4c 20 43 4f 4d 4d 45 4e 54 20 4f 54 48 45 52   JL COMMENT OTHER
000000b0:  20 3d 20 22 30 43 30 32 30 31 37 37 30 30 30 30    = "0C0201770000
000000c0:  30 30 30 30 30 30 37 37 30 30 30 30 30 30 30 30   0000007700000000
000000d0:  30 30 30 30 22 0d 0a 40 50 4a 4c 20 43 4f 4d 4d   0000"..@PJL COMM
000000e0:  45 4e 54 20 52 50 4a 4c 2c 57 49 4e 32 30 30 30   ENT RPJL,WIN2000
000000f0:  2c 50 43 4c 35 43 2c 31 2e 32 2e 30 2e 30 2c 43   ,PCL5C,1.2.0.0,C
00000100:  4f 4c 4f 52 0d 0a 40 50 4a 4c 20 4a 4f 42 20 4e   OLOR..@PJL JOB N
00000110:  41 4d 45 3d 22 4d 69 63 72 6f 73 6f 66 74 20 57   AME="Microsoft W
00000120:  6f 72 64 20 2d 20 74 65 73 74 35 5f 31 31 5f 32   ord - test5_11_2
00000130:  30 31 5f 6c 70 72 5f 70 63 6c 2e 64 6f 63 22 0d   01_lpr_pcl.doc".
00000140:  0a 40 50 4a 4c 20 53 45 54 20 4a 4f 42 4e 41 4d   .@PJL SET JOBNAM
00000150:  45 3d 22 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72   E="Microsoft Wor
00000160:  64 20 2d 20 74 65 73 74 35 5f 31 31 5f 32 30 31   d - test5_11_201
00000170:  5f 6c 70 72 5f 70 63 6c 2e 64 6f 63 22 0d 0a 40   _lpr_pcl.doc"..@
```

Figure 7c - Removing LPR data

5. Appendix

For readers with a further interest, we attached a network packet capture file ("testpcap.cap"). You can perform the operations demonstrated in this document by yourself.

Testpcap.cap

The capture contains packets sent by the following hosts:

PC1:	192.168.0.11
PC2:	192.168.0.12
printer1:	192.168.0.201
printer2:	192.168.0.202

During the capture, the following print jobs (1 page MS Word files) were submitted:

Job no.	PC>printer	Job type (port)	Lang.	Time
1.	11>201	DIPRINT(9100)	PCL5	x3
2.	12>201	DIPRINT(9100)	PS	x1
3.	11>202	DIPRINT(9100)	PCL5	x1
4.	12>202	DIPRINT(9100)	PS	x1
5.	11>201	LPR(515)	PCL5	x3
6.	12>201	LPR(515)	PS	x1
7.	11>202	LPR -d(515)	PCL5	x1
8.	12>202	LPR -d(515)	PS	x1

The packet capture is unfiltered and therefore also contains other network activity such as Pings.

NOTE: *When you are looking at LPR packets, the port number of the printer might be displayed as "printer", not "515". To change this, disable [View] > [Name Resolution] > [Enable Transport layer], then click [View] > [Reload] to reload the file.*