Taming the (Wire)Shark -Looking at Network Traces in a New Fashion Hands-on Lab

Matthias Burkhard
IBM Germany
mburkhar@de.ibm.com

Session 10828

March 14, 2012: 04:30 PM - 05:30 PM, OMNI, Pine

Session Contents 10828
Taming the (Wire)Shark -
Looking at Network Traces in a New Fashion

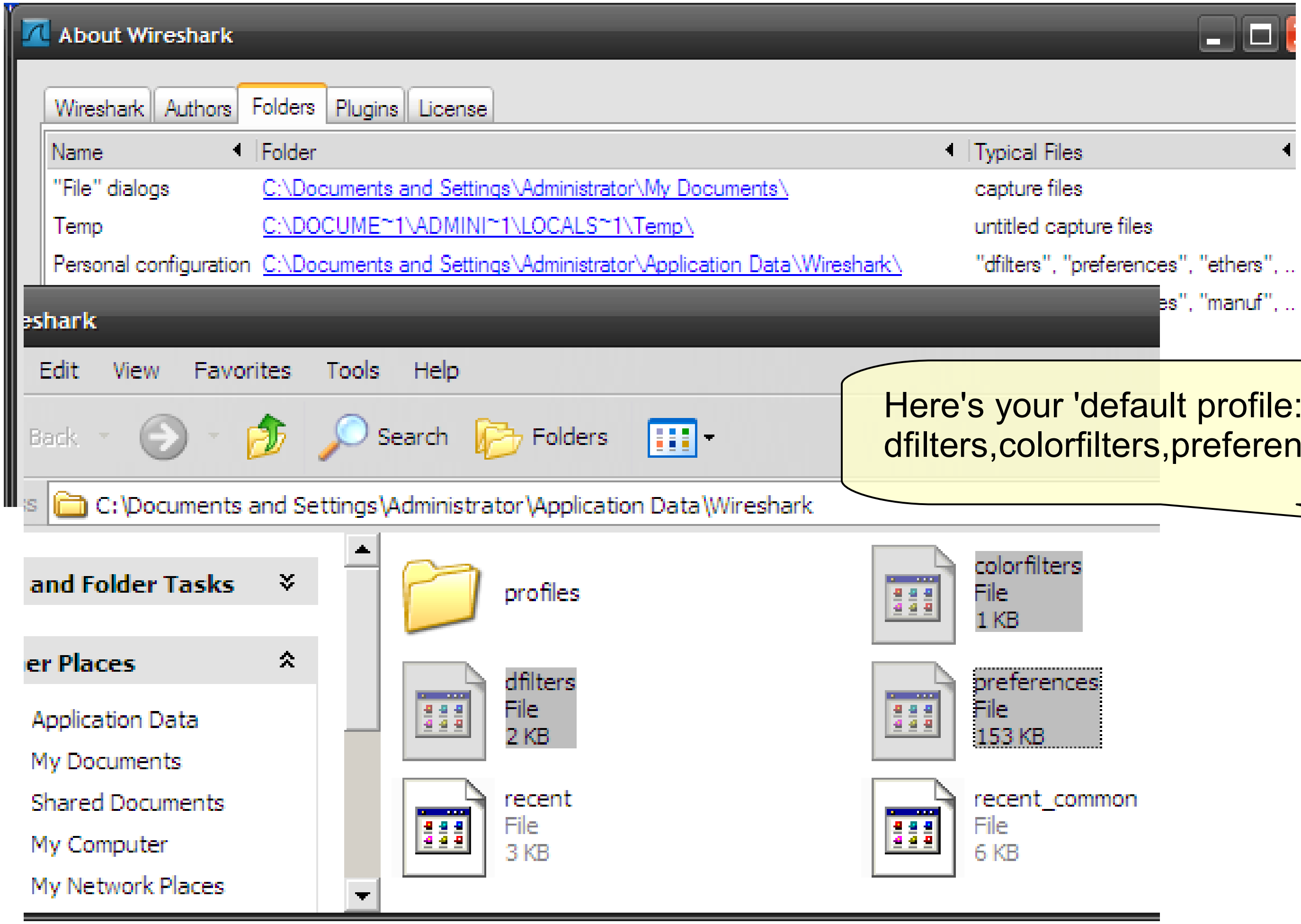
Session 10828: Taming the Shark
You have used wireshark before and found it valuable in your job as a z/OS TCPIP System Administrator?
Chances are, you've just scratched at the tip of the iceberg.
Come to this session to gain some hands-on experience and see how you really save time in trouble shooting by using some not-so-obvious filters, coloring rules and graphical features of the wireshark tool.

You're invited to bring and use your own computer to look at some trace examples showing real TCP/IP problems.

The Labs are based on Wireshark for Windows: Version 1.6.5

Installation Folders – Personal Configuration

- About Wireshark → Folders



Name	Folder	Typical Files
"File" dialogs	C:\Documents and Settings\Administrator\My Documents\	capture files
Temp	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\	untitled capture files
Personal configuration	C:\Documents and Settings\Administrator\Application Data\Wireshark\	"dfilters", "preferences", "ethers", ..
		es", "manuf", ..

C:\Documents and Settings\Administrator\Application Data\Wireshark

profiles

colorfilters
File
1 KB

dfilters
File
2 KB

preferences
File
153 KB

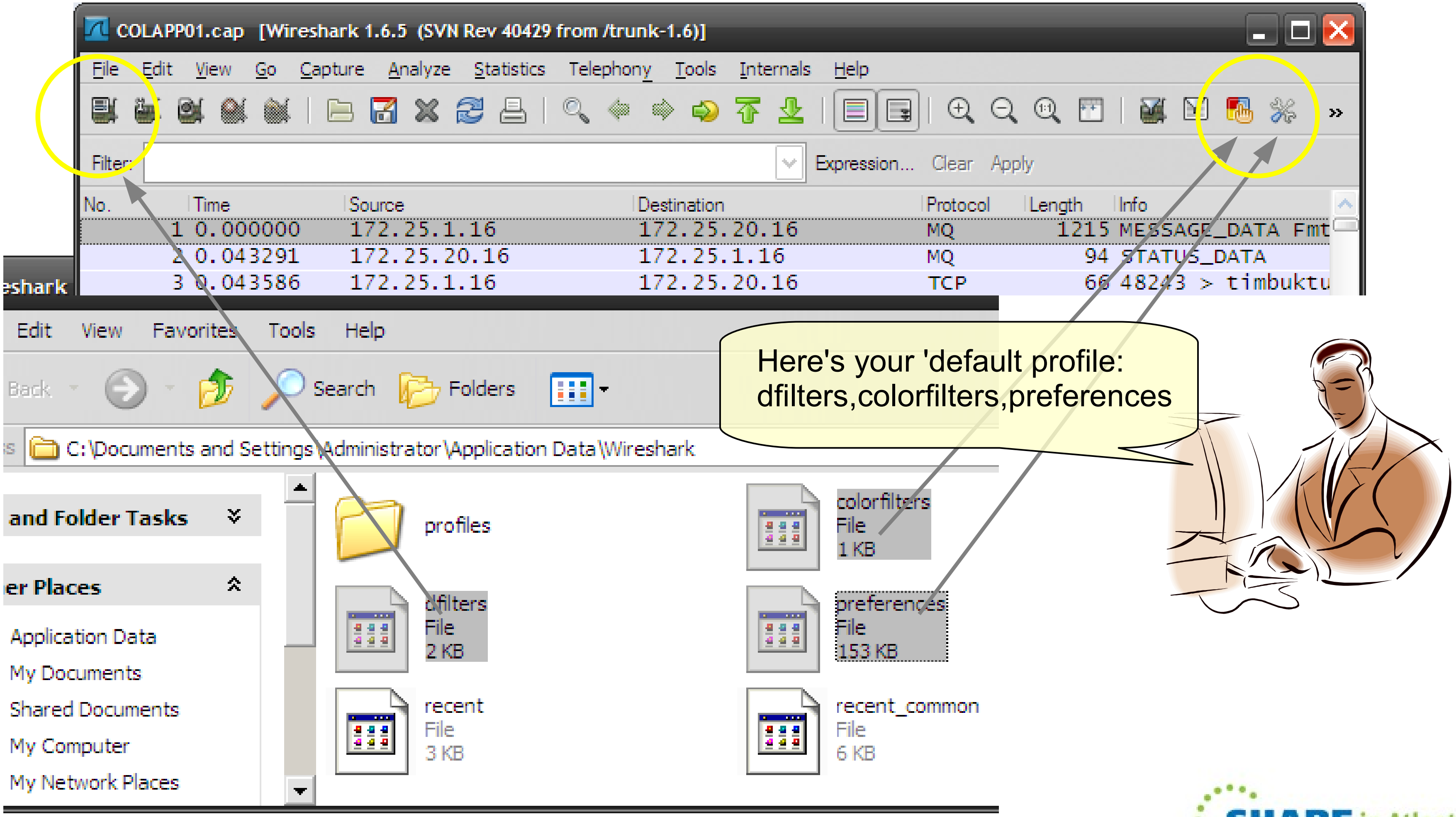
recent
File
3 KB

recent_common
File
6 KB

Here's your 'default profile:
dfilters,colorfilters,preferences

Profiles

- Default Profile



COLAPP01.cap [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

```
No.  Time       Source         Destination    Protocol  Length  Info
   1 0.000000   172.25.1.16    172.25.20.16   MQ          1215  MESSAGE_DATA Fmt
   2 0.043291   172.25.20.16   172.25.1.16    MQ            94  STATUS_DATA
   3 0.043586   172.25.1.16    172.25.20.16   TCP           66  48243 > timbuktu
```

C:\Documents and Settings\Administrator\Application Data\Wireshark

profiles	colorfilters File 1 KB
dfilters File 2 KB	preferences File 153 KB
recent File 3 KB	recent_common File 6 KB

Here's your 'default profile:
dfilters,colorfilters,preferences

WebSphere MQ Timeout Problem

- Understand Problem
  - What is the concern?
  - What is the impact?
  - What is the root cause?

```
AMQ9259: Connection timed out from host '172.25.1.16'.
AMQ9999: Channel program ended abnormally.
EXPLANATION:
Channel program 'CRDB.PXS.TCP' ended abnormally.
```

AMQ9259, AMQ9999
Let's get started...

- Understand the Topology
  - What Platforms are involved?
  - What does the Network Infrastructure look like?
  - What TCP/IP parameters are configured?

- Evaluate possible Solutions
  - Ease of implementation
  - Scope of responsibility

CICS Transaction Gateway Timeout Problem

```
CTG Client:
CCL4446E TCP/IP TCP/IP send()
         API call timed out (errno = ETIMEDOUT)
CCL4414E TCP/IP (to CTGSRV01) link failed: RC=10060
```

- Understand Problem
  - What is the concern?
  - What is the impact?
  - What is the root cause?
- Understand the Topology
  - What Platforms are involved?
  - What does the Network Infrastructure look like?
  - What TCP/IP parameters are configured?
- Evaluate possible Solutions
  - Ease of implementation
  - Scope of responsibility

CTG: ETIMEDOUT
The CCL4446E message is issued when the client daemon tries to send data to a CICS server over the TCP/IP protocol, but the TCP send does not complete within 5 seconds.

Thank You for your time!

Matthias Burkhard
IBM
mburkhar@de.ibm.com

Twitter : mreede

IP Wizards

ip.wizards@groups.facebook.com

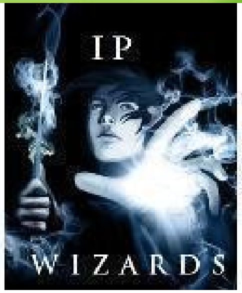
EE Education – IP wizards

ITS53 EE Implementation and Problem Determination

4 days ITSO Workshop – 30.April 2012 Miami,FL

Register at http://greenhouse.lotus.com

Join the IP wizards community



http://tinyurl.com/ipwizards

to download wireshark profiles and p0f fingerprints