Wireshark Developer and User Conference

Customizing Wireshark for Different Use Scenarios

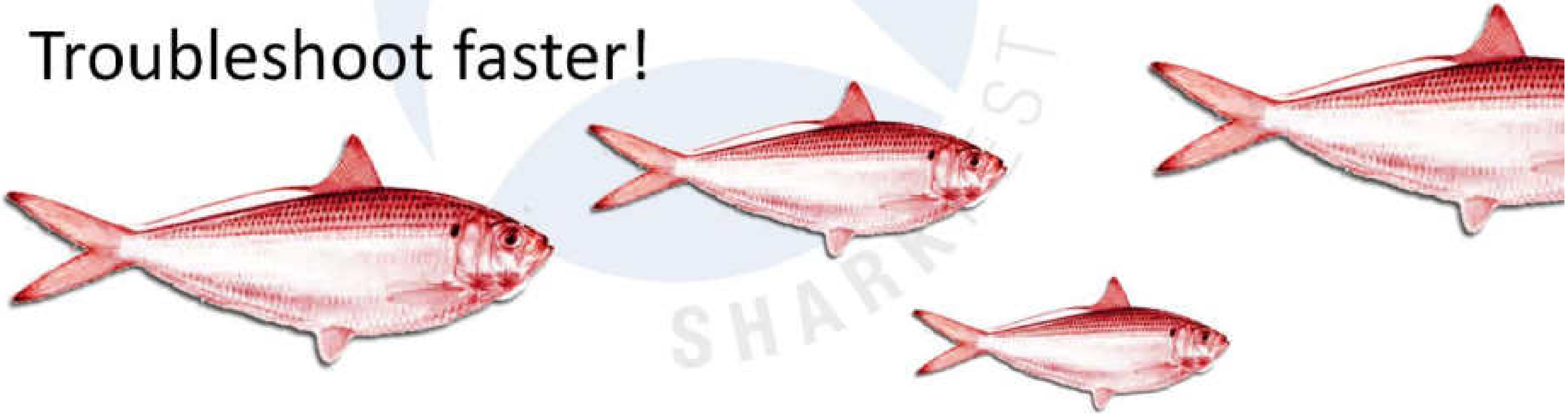
June 14, 2011

Laura Chappell
Founder | Chappell University/Wireshark University
laura@chappellU.com

SHARKFEST **'11**
Stanford University
June 13-16, 2011

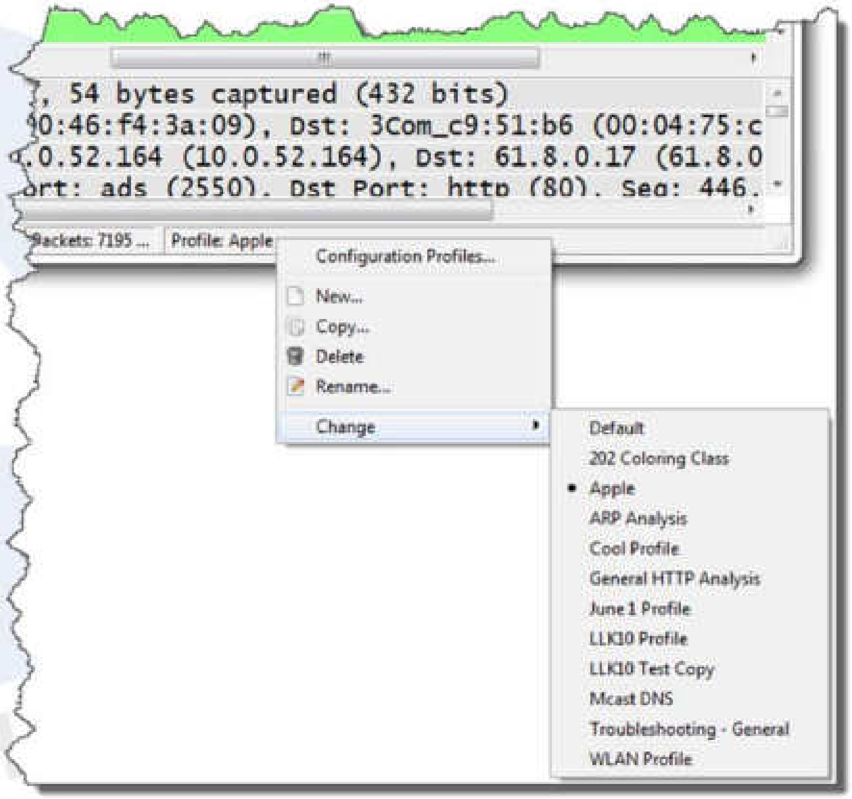
Why Customize

- Call attention to potential issues
- Provide more information in the Packet List pane – fabulous!
- Alter current interpretations of traffic to remove "red herrings"
- Troubleshoot faster!



Overview of Profiles

- Where they reside
- What they contain
- How to share them
- Some samples of use
- Where you can get a pre-made profile

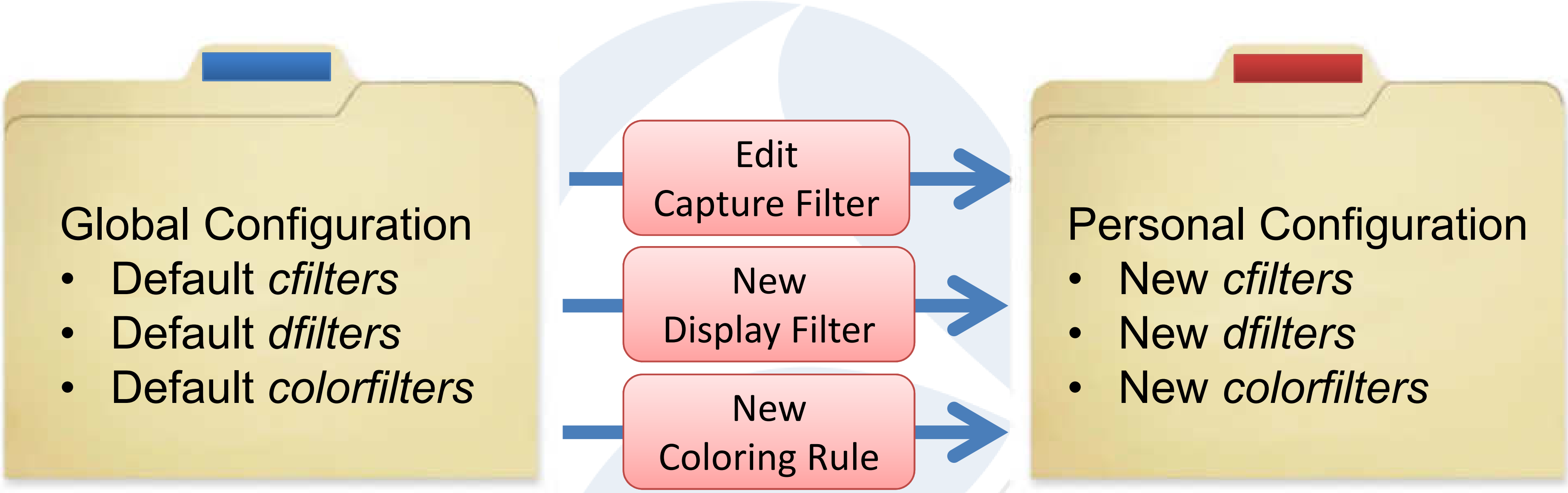


```
, 54 bytes captured (432 bits)
0:46:f4:3a:09), Dst: 3Com_c9:51:b6 (00:04:75:c
.0.52.164 (10.0.52.164), Dst: 61.8.0.17 (61.8.0
ort: ads (2550), Dst Port: http (80), Seq: 446,
```

Where Do Profiles Fit?

Wireshark Program
File Folder*

Personal Configuration
File Folder*



Global Configuration
- Default *cfilters*
- Default *dfilters*
- Default *colorfilters*

Edit
Capture Filter

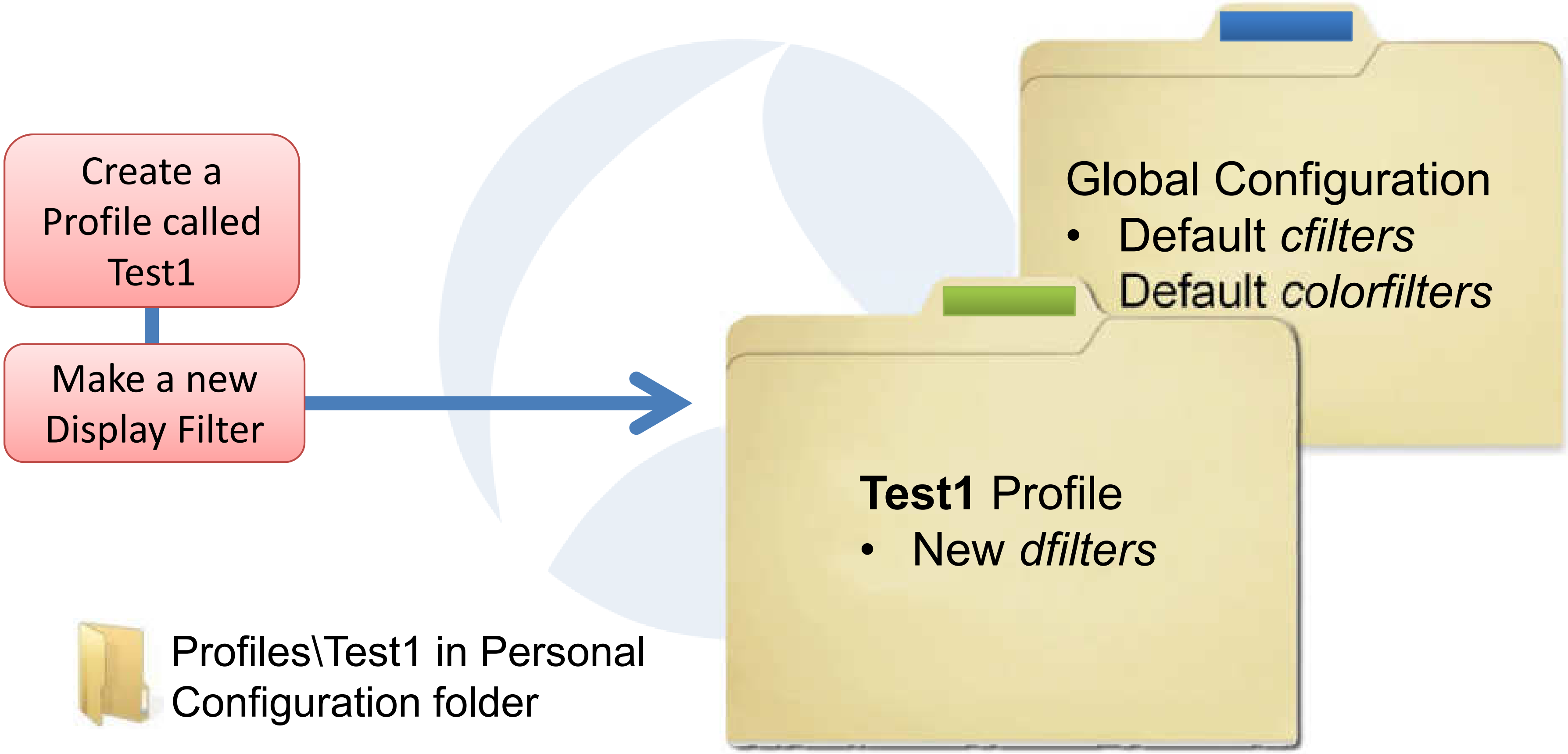
New
Display Filter

New
Coloring Rule

Personal Configuration
- New *cfilters*
- New *dfilters*
- New *colorfilters*

*Select Help | About Wireshark | Folders to locate

Where Do Profiles Fit?



Create a Profile called Test1

Make a new Display Filter

Global Configuration

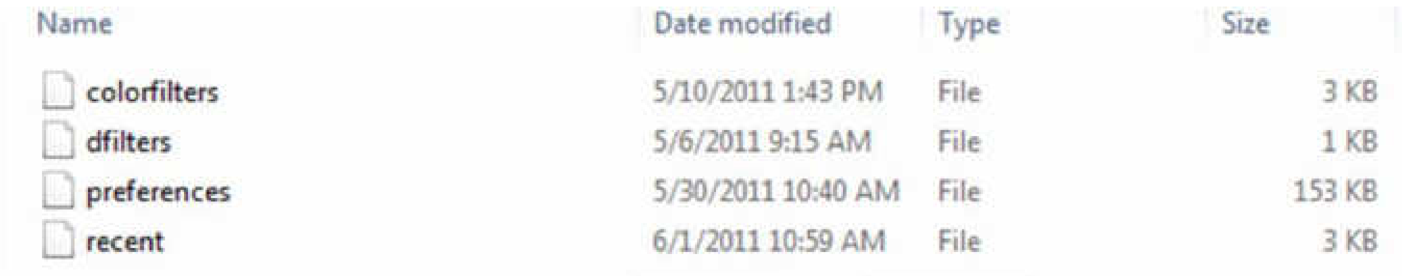
- Default *cfilters*
- Default *colorfilters*

Test1 Profile

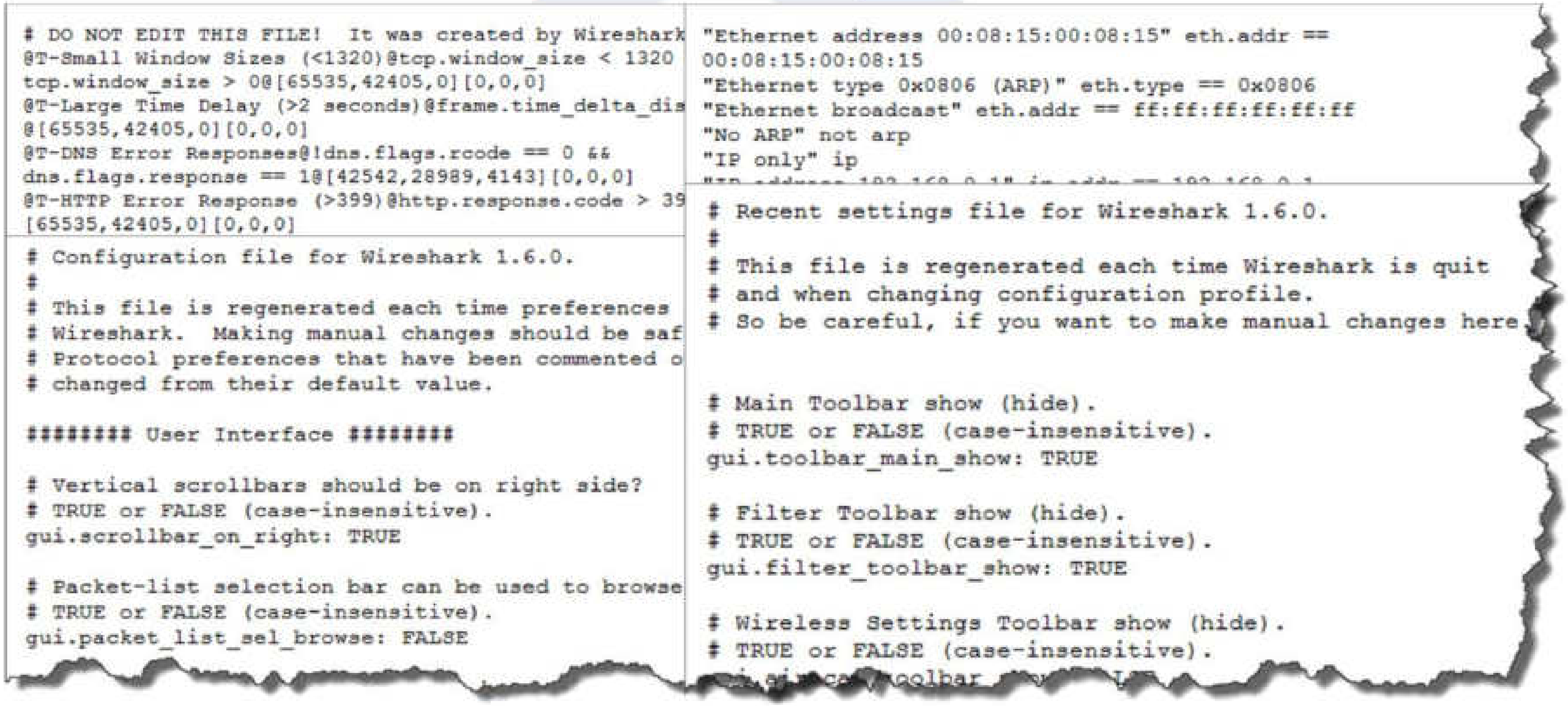
- New *dfilters*

Profiles\Test1 in Personal Configuration folder

Some Profile Elements



Name	Date modified	Type	Size
colorfilters	5/10/2011 1:43 PM	File	3 KB
dfilters	5/6/2011 9:15 AM	File	1 KB
preferences	5/30/2011 10:40 AM	File	153 KB
recent	6/1/2011 10:59 AM	File	3 KB



```
# DO NOT EDIT THIS FILE!  It was created by Wireshark
@T-Small Window Sizes (<1320)@tcp.window_size < 1320
tcp.window_size > 0@[65535,42405,0][0,0,0]
@T-Large Time Delay (>2 seconds)@frame.time_delta_dis
@[65535,42405,0][0,0,0]
@T-DNS Error Responses@!dns.flags.rcode == 0 &&
dns.flags.response == 1@[42542,28989,4143][0,0,0]
@T-HTTP Error Response (>399)@http.response.code > 39
[65535,42405,0][0,0,0]
```

```
# Configuration file for Wireshark 1.6.0.
#
# This file is regenerated each time preferences
# Wireshark.  Making manual changes should be saf
# Protocol preferences that have been commented o
# changed from their default value.

######## User Interface ########

# Vertical scrollbars should be on right side?
# TRUE or FALSE (case-insensitive).
gui.scrollbar_on_right: TRUE

# Packet-list selection bar can be used to browse
# TRUE or FALSE (case-insensitive).
gui.packet_list_sel_browse: FALSE
```

```
"Ethernet address 00:08:15:00:08:15" eth.addr ==
00:08:15:00:08:15
"Ethernet type 0x0806 (ARP)" eth.type == 0x0806
"Ethernet broadcast" eth.addr == ff:ff:ff:ff:ff:ff
"No ARP" not arp
"IP only" ip
"IP address 192.168.0.1" ip.addr == 192.168.0.1
```

```
# Recent settings file for Wireshark 1.6.0.
#
# This file is regenerated each time Wireshark is quit
# and when changing configuration profile.
# So be careful, if you want to make manual changes here.


# Main Toolbar show (hide).
# TRUE or FALSE (case-insensitive).
gui.toolbar_main_show: TRUE

# Filter Toolbar show (hide).
# TRUE or FALSE (case-insensitive).
gui.filter_toolbar_show: TRUE

# Wireless Settings Toolbar show (hide).
# TRUE or FALSE (case-insensitive).
gui.airpcap_toolbar_show: TRUE
```

Starting from "Scratch"

- Creating your first profile (master)
- Adding key settings

Recommended Key Settings

- Disable “Checksum Errors” coloring rule
- Create new coloring rule for Window Update packets – these are good!

Recommended Key Settings

- Add “butt ugly” coloring rules for TCP Option problems –
  - the 4 EOL issue
  - the 4 NOP issue
- Add “butt ugly” for low Window Size value and Window Scale factor of 0

Time Setting

- Good:
  - Time Column Setting as Delta Displayed
- Better:
  - Custom Column: tcp.time_delta
  - Requires “Calculate Conversation Timestamp” in TCP protocol setting
  - Consider a “butt ugly” coloring rule too (> 1.0?)

Let’s check this out!

Protocol Settings

- Checksum necesssary?
- Extra ports for HTTP?
- Keys?

Let’s check this out!

Let’s Add to our Profile

Remember – Laura’s Lab Kit v10
has a troubleshooting profile
and video training on creating and
importing that profile
(download the ISO at lcuportal.com)

New Projects

Often the result of boredom and bad weather