

Today's handouts can be  
downloaded today from the  
ChappellU Portal at  
[lcpuportal2.com](http://lcpuportal2.com)



## Wireshark Network Analysis

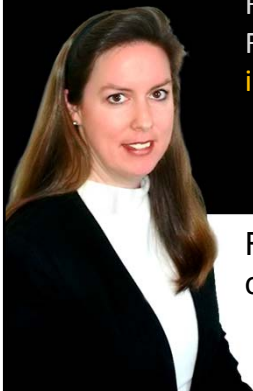
The Official Wireshark Certified Network Analyst Study Guide

“In short, whether you are on the air or wire there is no better tool than Wireshark and there is no better book than this...!”

SecurityXploded.com  
Awarded “Book of the Month”

## Presenter: Laura Chappell

Founder, Chappell University ([chappellU.com](http://chappellU.com))  
Founder, Wireshark University ([wiresharkU.com](http://wiresharkU.com))  
[info@chappellU.com](mailto:info@chappellU.com)



For sample trace files, videos and  
configuration files, visit [wiresharkbook.com](http://wiresharkbook.com)



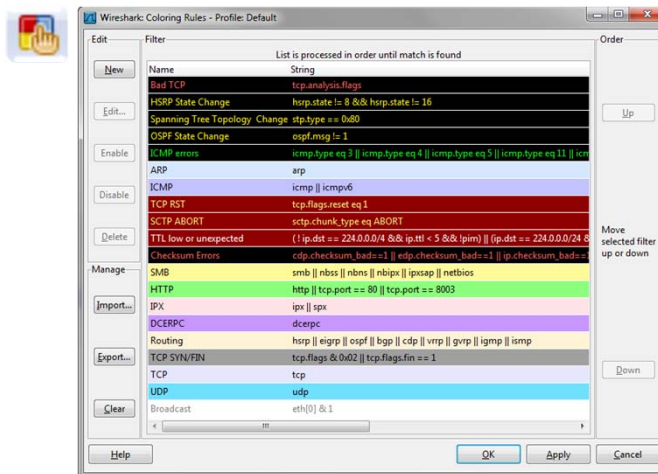
(c) Chappell University 2011

# Our Focus Today

- ▶ Default Coloring Rules
- ▶ Disable All/Single Coloring Rules
- ▶ Conversation Coloring
- ▶ Add New Coloring Rules [Best Practices]
- ▶ Sample Coloring Rules to Add
- ▶ Work with Coloring in Profiles
- ▶ Edit the *colorfilters* Text File
- ▶ Share Coloring Rules

(c) Chappell University 2011

# 20 Default Coloring Rules



(c) Chappell University 2011

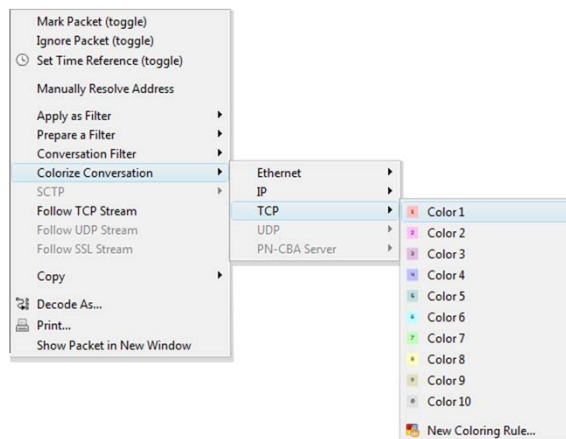
## Disabling Coloring Rules

- Why disable coloring rules?
- Disabling all rules
- Disabling single coloring rules
- Restoring the default coloring rule set

(c) Chappell University 2011

## Separating Conversations

- http-espn2010.pcap and voip-extension.pcap
- 10 colors
- Coloring is only temporary unless you choose “New Coloring Rule...”



(c) Chappell University 2011

## New Coloring Rules – Best Practices

- Excessive coloring rules can **slow down** Wireshark processing
- Coloring rules are processed **top to bottom**
- Separate coloring rules in **profiles**
- Define a **coloring scheme**
- Use **coloring names** (often hex)
- Use a **sortable naming convention**

(c) Chappell University 2011

## Sample Troubleshooting Coloring Rules

- High latency between packets
- Error responses
- Inefficient packet sizes

Consider adding security-related coloring rules as well.

(c) Chappell University 2011

## Sample Troubleshooting Coloring Rules

- @T-High Delta Display Time (adjust as needed)@tcp.time\_delta > 0.500000000@[63479,41891,21588][0,0,0]
- @T-DHCP NACK (DHCP Server Does Not Like Target)@(bootp.option.type == 53) && (bootp.option.value == 06)@[63479,41891,21588][0,0,0]
- @T-HTTP Error Code@http.response.code > 299 @[63479,41891,21588][0,0,0]
- @T-ICMP Type 3/Code 4 (Black Hole Detection?)@icmp.type == 3 and icmp.code == 4@[63479,41891,21588][0,0,0]

(c) Chappell University 2011

## Sample Troubleshooting Coloring Rules

- @T-PPI Signal < -80 (Weak Signal Strength at Antenna Location)@ppi.80211-common.dbm.antsignal < -80@[63479,41891,21588][0,0,0]
- @T-RadioTap Signal < -80 (Weak Signal Strength at Antenna Location)@radiotap.dbm\_antsignal < -80@[63479,41891,21588][0,0,0]
- @T-SIP Error Responses@sip.Status-Code >= 300@[63479,41891,21588][0,0,0]
- @T-TCP Length == 536 (MTU Issue Along Path?)@tcp.len==536@[63479,41891,21588][0,0,0]

(c) Chappell University 2011

## Coloring in Profiles

- Example of Profiles
  - VoIP
  - WLAN
  - Corporate office
  - HTTP
  - Other application

(c) Chappell University 2011

## The *colorfilters* File

- Simple text file
- Contains a warning not to edit
- You *CAN* edit this file with caution

```
# DO NOT EDIT THIS FILE! It was created by Wireshark
@Bad TCP@tcp.analysis.flags@[0,0,0][65535,24383,24383]
@HSRP State Change@hsrp.state != 8 && hsrp.state != 16@[0,0,0]
[65535,63222,0]
@Spanning Tree Topology Change@stp.type == 0x80@[0,0,0][65535,63222,0]
@OSPF State Change@ospf.msg != 1@[0,0,0][65535,63222,0]
@ICMP errors@icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 ||
icmp.type eq 11@[0,0,0][0,65535,3616]
@ARP@arp@[55011,59486,65534][0,0,0]
@ICMP@icmp || icmpv6@[49680,49737,65535][0,0,0]
@TCP RST@tcp.flags.reset eq 1@[37008,0,0][65535,63121,32911]
@TTL low or unexpected@( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim)
|| (ip.dst == 224.0.0.0/24 && ip.ttl != 1)@[37008,0,0]
[65535,65535,65535]
@Checksum Errors@udp.checksum_bad==1 || edp.checksum_bad==1 ||
ip.checksum_bad==1 || tcp.checksum_bad==1 || udp.checksum_bad==1 ||
mstp.checksum_bad==1@[0,0,0][65535,24383,24383]
@SMB@ smb || nbns || nbns || nbns || ipxap || netbios
```

(c) Chappell University 2011

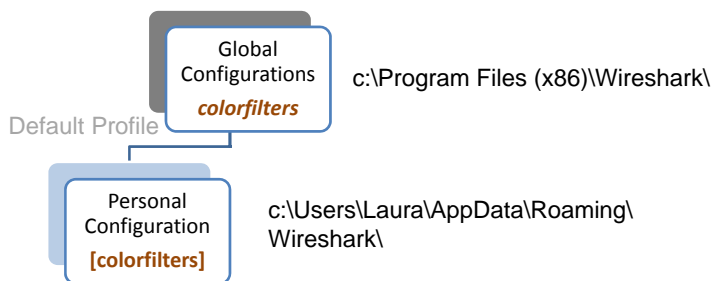
## How *colorfilters* is Created

Global  
Configurations  
*colorfilters*

c:\Program Files (x86)\Wireshark\

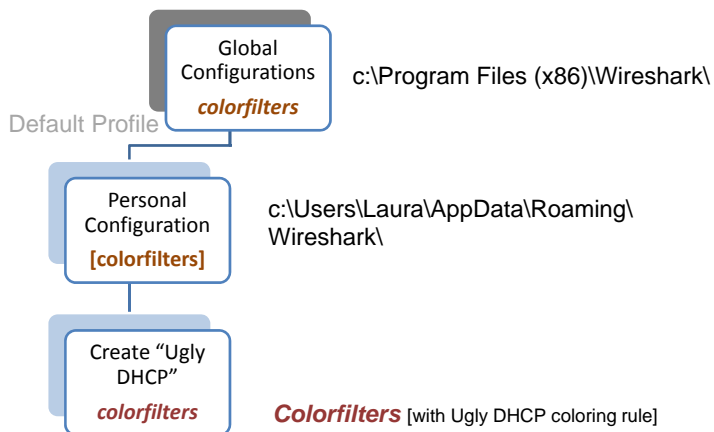
(c) Chappell University 2011

## How *colorfilters* is Created



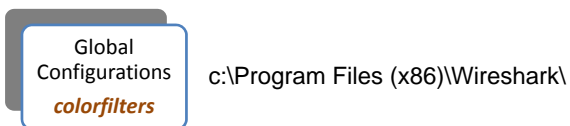
(c) Chappell University 2011

## How *colorfilters* is Created



(c) Chappell University 2011

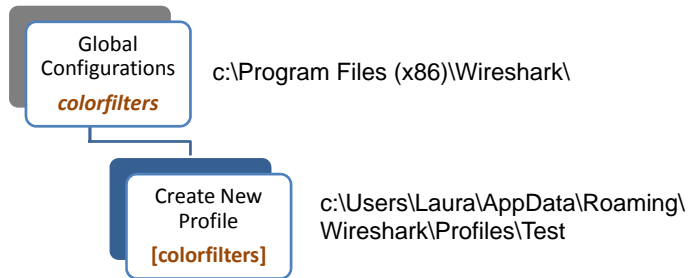
## How *colorfilters* is Created



(c) Chappell University 2011

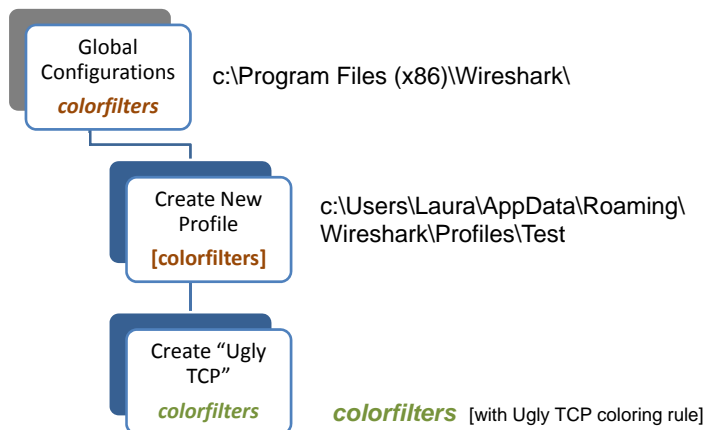


## How *colorfilters* is Created



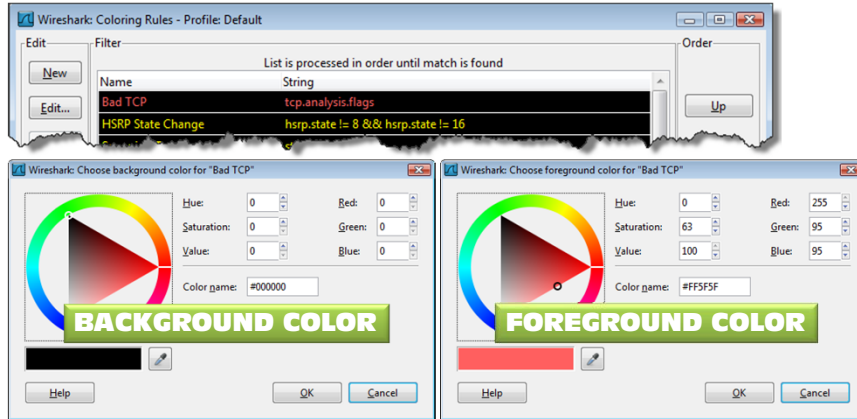
(c) Chappell University 2011

## How *colorfilters* is Created



(c) Chappell University 2011

## How colorfilters is Created

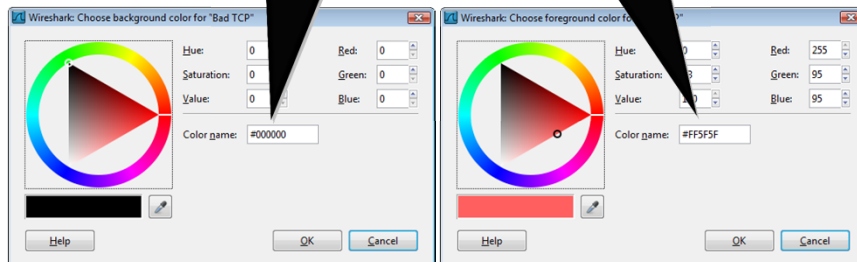


@Bad TCP@tcp.analysis.flags@[0,0,0][65535,24383,24383]

(c) Chappell University 2011

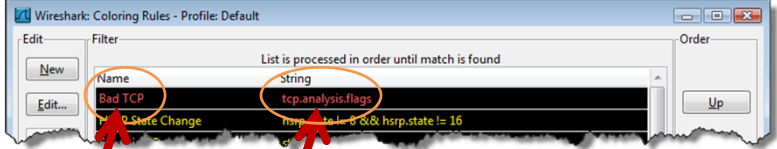
## How colorfilters is Created

You can enter a color name such as red, blue, green, yellow, light blue, light green, black, grey, etc.



(c) Chappell University 2011

## How colorfilters is Created

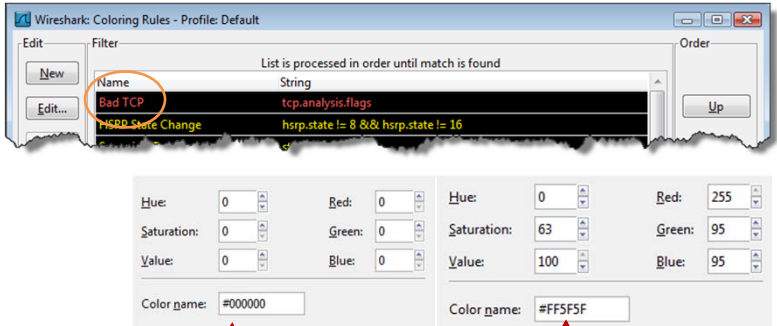


The screenshot shows the 'Wireshark: Coloring Rules - Profile: Default' dialog. A table lists rules with columns for Name and String. The rule 'Bad TCP' is highlighted, with its filter expression 'tcp.analysis.flags' circled in red. Red arrows point from the 'Name' and 'String' columns to a table below.

Name	String
@Bad TCP	@tcp.analysis.flags@[0,0,0][65535,24383,24383]

(c) Chappell University 2011

## How colorfilters is Created



The screenshot shows the same 'Wireshark: Coloring Rules' dialog as above, but with two color selection panels below. The first panel shows a color selection for the 'Bad TCP' rule, with the 'Color name' field set to '#000000'. The second panel shows a color selection for the filter expression, with the 'Color name' field set to '#FF5F5F'. Red arrows point from these color names to the corresponding parts of the filter expression in the table below.

@Bad TCP	@tcp.analysis.flags@[0,0,0]	[65535,24383,24383]
		[0xFF] [0x5F] [0x5F]

(c) Chappell University 2011

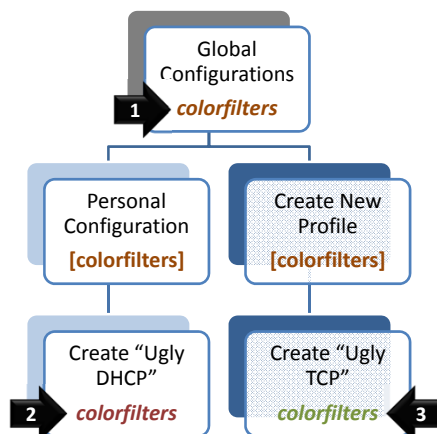
## Let's Manually Add Coloring Rules



- Open in text editor
- Copy/paste existing filter to new line
- Edit name/string and color settings
- Use “!” before a coloring rule to disable it

(c) Chappell University 2011

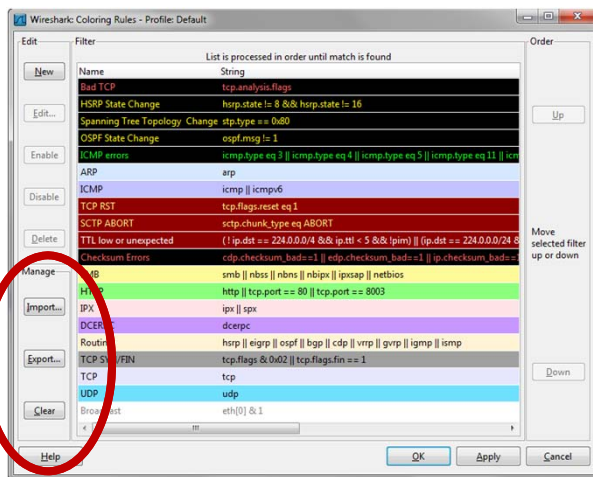
## Sharing a *colorfilters* File



- Which colorfilters file do you want to share?
- Or do you want to share one coloring rule alone?

(c) Chappell University 2011

## Sharing a *colorfilters* File



(c) Chappell University 2011

# Questions?

[www.chappellU.com](http://www.chappellU.com)  
[info@chappellU.com](mailto:info@chappellU.com)

(c) Chappell University 2011