

Stylin' with Wireshark Profilin'



Josh Clark
Huntington National Bank

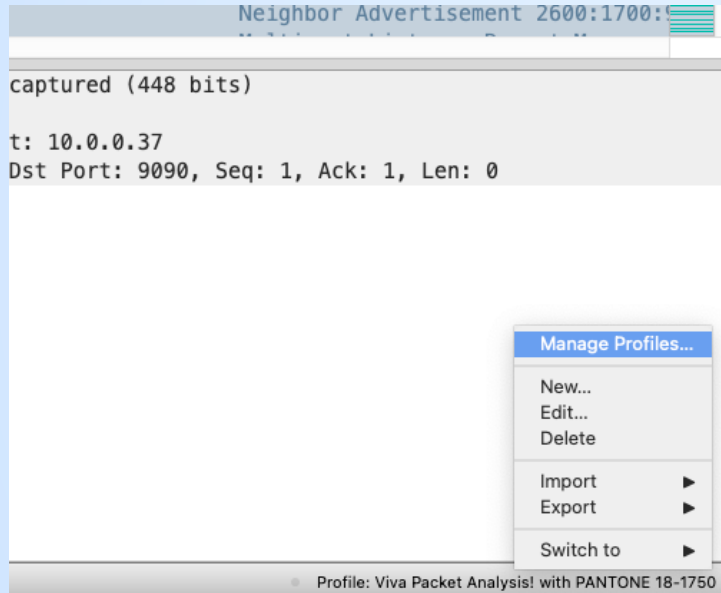


Who Am I?

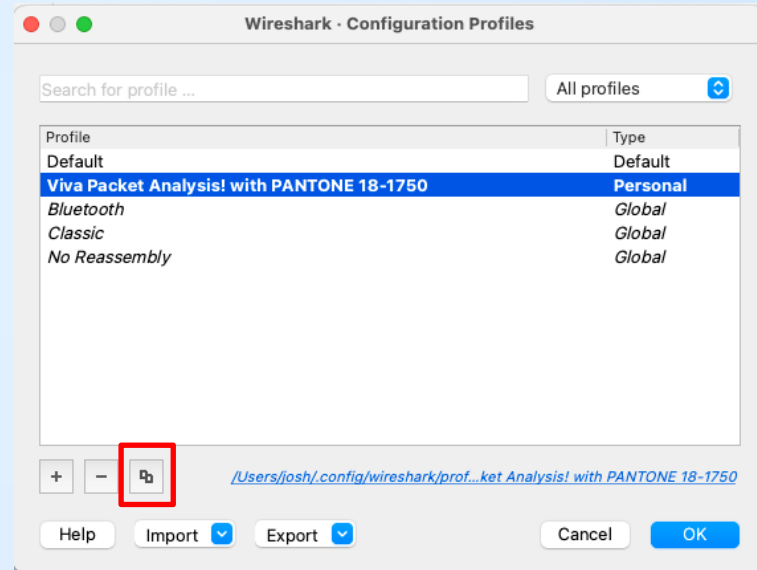
- ① Developed Pantone Color of the Year Wireshark Profiles - 2021-now
 - https://github.com/je-clark/wireshark_profiles
- ① Distributed Performance Engineer - 2018-now
- ① M.S. in Network Engineering - 2016



Manage Profiles and Duplicate a Profile



Right-click on Profile



Click the duplicate button to create a copy of a profile

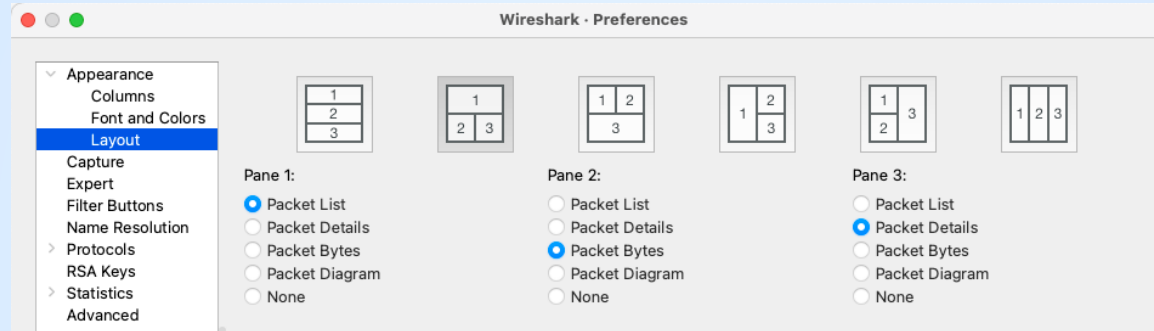


What's the Goal?

- ① Think critically about your analysis workflows
- ① Learn what helps YOU understand captures
- ① Create a new default profile that suits YOU

My job is to give you some examples

Layout



Preferences -> Appearance -> Layout

I prefer Packet Bytes on the left and Packet Details on the right to reduce visual distance between questions in the packet list and answers in the bytes or details



Columns - Timing Data

Time Display Format	>	Date and Time of Day (1970-01-01 01:02:03.123456)	⌘ 1
Name Resolution	>	Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)	
Zoom	>	Time of Day (01:02:03.123456)	⌘ 2
Expand Subtrees	⇧ ▶	Seconds Since 1970-01-01	⌘ 3
Collapse Subtrees	⇧ ◀	✓ Seconds Since First Captured Packet	⌘ 4
Expand All	⌘ ▶	Seconds Since Previous Captured Packet	⌘ 5
		Seconds Since Previous Displayed Packet	⌘ 6

In View -> Time Display Format, select “Seconds Since First Captured Packet”

This enables quick use of “Set Time Reference”



Columns - Timing Data

Wireshark · Preferences



Displayed	Title	Type	Fields	Field Occurrence	Resolved
<input checked="" type="checkbox"/>	No.	Number			
<input checked="" type="checkbox"/>		Time (format as specified)			
<input checked="" type="checkbox"/>	Arrival Time	Custom	frame.time	0	
<input checked="" type="checkbox"/>	Δ Disp	Custom	frame.time_delta_displayed	0	
<input checked="" type="checkbox"/>	Δ Conv	Custom	tcp.time_delta or udp.time_delta	0	

- Add a separate **Arrival Time** column for readable date and time
- **Delta Display** shows inter-packet time in the display filter context
- **Delta Conversation** shows inter-packet time in the conversation context



Columns - Default Frame Data

#sf23us

Name Resolution	<input checked="" type="checkbox"/>	Source	Source address		
> Protocols	<input checked="" type="checkbox"/>	Destination	Destination address		
RSA Keys	<input checked="" type="checkbox"/>	Protocol	Protocol		
> Statistics	<input checked="" type="checkbox"/>		Custom	tcp.len or udp.length	0
Advanced	<input checked="" type="checkbox"/>		Custom	tcp.flags.str or dns.flags	0

- **Source**, **Destination**, **Protocol**, and **Info** are useful defaults
- **Length** shows TCP or UDP payload length
- **Flags** shows TCP or DNS flags in a compact format

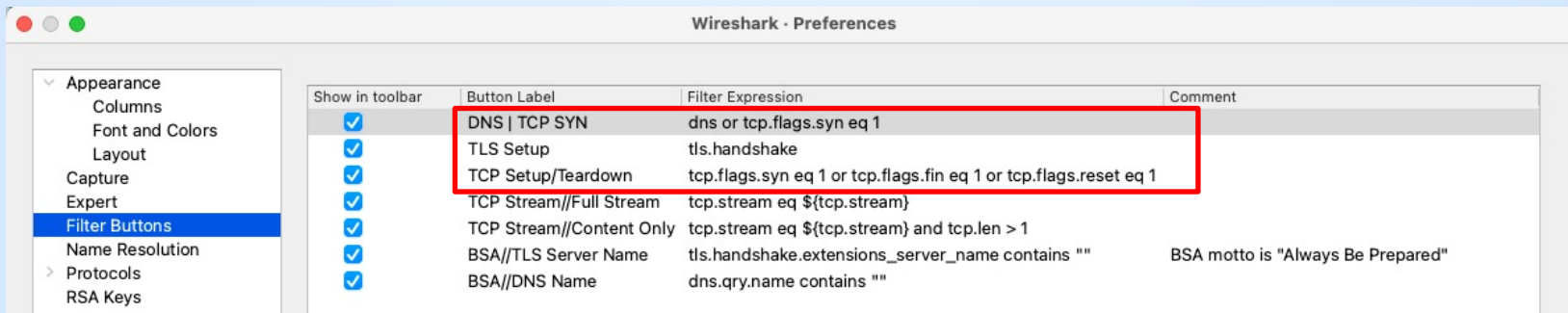


Columns - Deep Dive Hidden by Default

<input type="checkbox"/>	Seq	Custom	tcp.seq	0
<input type="checkbox"/>	Next Seq	Custom	tcp.nxtseq	0
<input type="checkbox"/>	Ack	Custom	tcp.ack	0
<input type="checkbox"/>	Server Name	Custom	tls.handshake.extensions_server_name	0
<input type="checkbox"/>	Name	Custom	dns.qry.name	0
<input type="checkbox"/>	Stream index	Custom	tcp.stream	0

- **Seq**, **Next Seq**, and **Ack** are crucial for TCP analysis
- **TLS Server Name** and **DNS Name** give clues towards active services
- **Stream Index** works as a 'sort-by' column for concurrent connections

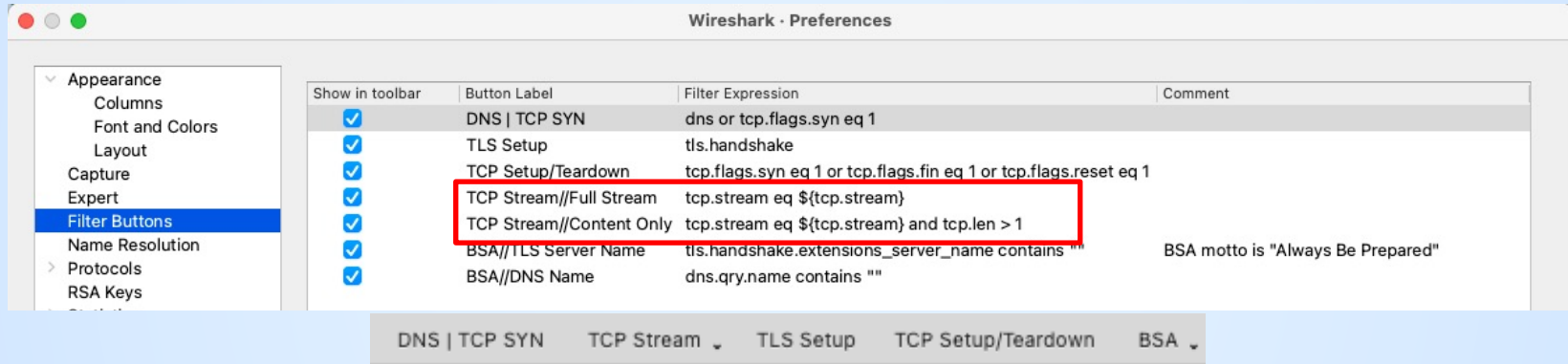
Display Filter Buttons - Orienting Yourself



- **DNS or SYN** connects service name to IP better than reverse lookup when SaaS services are in play
- **TLS Setup** can quickly identify services and hosts when using the TLS Server Name column
- **TCP Setup/Teardown** gives you context on long and short TCP conversations when sorting by Stream Index and looking at Delta Display



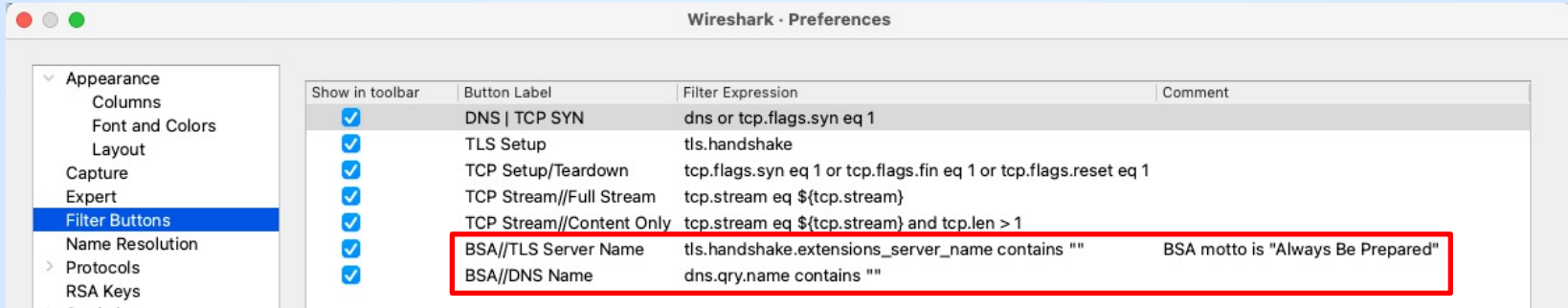
Display Filter Buttons - Deep Dive



- The format “Parent//child” creates a dropdown menu where labels with common parents are grouped
- Full Stream applies the TCP Stream Index of the current packet to the display filter
 - It functions as a shortcut to Right Click on Packet -> Follow Stream
- Content Only ignores ACKs, keepalives, and other noise



Display Filter Buttons - Prepare As



- These buttons are **ALWAYS** used by Right Click -> Prepare as Filter
- TLS Server Name allows you to search for a domain name in the TLS Client Hello
- DNS Name allows you to search for a domain name in DNS Requests or Replies



Colors - Color Palette Resources

- A color palette is a set of colors used together
- <https://colorhunt.co/> lets you look through a bunch of palette options
- <https://colors.co/> lets you upload an image and automatically create a palette from it
- <https://color.adobe.com/create/color-wheel> lets you refine a palette using color theory



Colors - Color Wheel



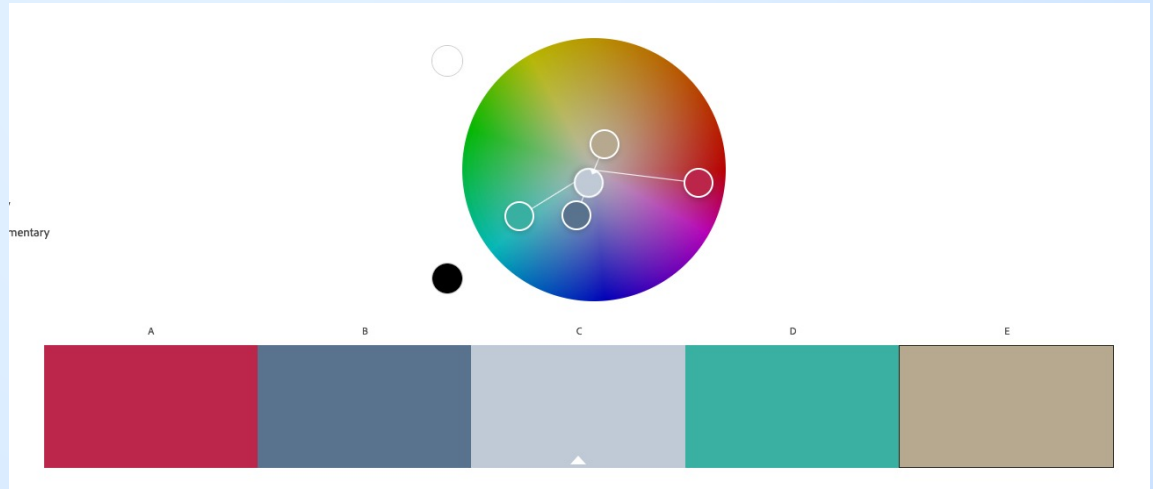


Colors - Color Harmony Rules

- **Analogous** – Next to each other
- **Monochromatic** – On a shared radius
- **Complementary** – On a shared diameter
- **Triadic** – Roughly 120 deg apart
- **Split Complementary** – Equally far away from a shared diameter

Colors - My Formula

- 2 monochromatic base colors
- 1 complementary accent color
- 2 alert colors not quite split complementary from the primary diameter line





Colors - Base Coloring Rules

Name	Filter
<input checked="" type="checkbox"/> PANTONE 18-1750 Viva Mag...alysis leads you towards	tcp.time_delta gt 0.7
<input checked="" type="checkbox"/> DNS - PANTONE 15-1115 Fie...itions between OSI layers	dns
<input checked="" type="checkbox"/> TCP Setup/Teardown - PANT...d closing in conversation	tcp.flags.syn eq 1 or tcp.flags.reset eq 1 or tcp.flags.fin eq 1
<input checked="" type="checkbox"/> TLS Setup - PANTON 13-411...d closing in conversation	tls.handshake
<input checked="" type="checkbox"/> Bad TCP - PANTONE 18-1750...h and identify TCP errors	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
<input checked="" type="checkbox"/> PANTONE 13-4111 Plein Air ...iew normal network traffic	frame

- Use the monochromatic pair for frame
- Use the frame background color with white or black for TCP and TLS setup and teardown
- Use the accent color for dns
- Use the alert colors for whatever you need



Conclusion

When you build your own default profile, consider:

- What do you analyze most often?
- What are the most important protocols and fields to focus on?
- How can you reduce visual distance between important information?
- How can you reduce visual fatigue?
- What common tasks can you automate?

The logo for SharkFest'23 US features a blue circular emblem with a white shark fin cutting through it. To the right of the emblem, the text "SharkFest'23 US" is written in a bold, black, sans-serif font. Below this, "San Diego, CA • June 10-15" is written in a smaller, black, sans-serif font.

SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Questions?
