

Preferences

www.ine.com

Wireshark Preferences

» What can you change?

- Settings
- Look and feel
- Technical aspects such as NIC
- Other dynamics

Remember, preferences can be saved in profiles

• When you change preferences, you can match them up to specific profiles so you can save your changes



Configuring Preferences

Wireshark: Preferences - Pro	ofile: Use DNS Resolution	
User Interface		
Layout	Save window position:	
Columns	Save window size:	
Font and Colors	Save maximized state:	
Capture Filter Expressions	Check for updates:	V
Name Resolution		
Printing	Open a console window	Never
Protocols	"File Open" dialog behavior:	Remember last directory Always start in:
	Directory:	C:\Users\rshimonski\Documents
	"File Open" preview timeout:	3
	Maximum recent filters:	10
	Maximum recent files:	10
	Confirm unsaved capture files:	V
	Wrap to end/beginning of file during a find:	V
	Settings dialogs show a save button:	
	Welcome screen and title bar shows version	Both
	Auto scroll on expansion:	
	Auto scroll percentage:	0
	Display icons in the Expert Infos dialog tab labels:	
Help		<u>O</u> K <u>Apply</u> <u>Cancel</u>



Wireshark Preferences

» Adjusting look and feel

- Adjusting the user interface
- Layout adjustments
- Columns
- Fonts and colors
- » Adjusting capture specifics
 - Adjusting the user interface



Configuring Preferences

Wireshark: Preferences - Profile:	Use DNS Resolution		Notes and		
User Interface Layout Columns	Main window font:	Lucida Console Normal 10	Lazy badgers mo	ove unique waxy jellyfis	h packets 0123456789
Font and Colors Capture Filter Expressions Name Resolution	Colors:	'Follow Stream' client foreground	Sample marked pa Sample ignored p Sample 'Follow S Sample 'Follow S	acket text packet text Stream' client text Stream' server text	
Printing Protocols		Hue:	0	<u>R</u> ed: 127	
Statistics Stats Tree		Saturati	ion: 100 🛓	<u>G</u> reen: 0	
		Value: Opacity Color <u>n</u>		<u>Blue:</u> 0 <u>*</u> 255	
Help				<u>O</u> K	Apply Cancel



Copyright © www.ine.com

Wireshark Preferences

» Creating a new preference

- For this example, we will customize the columns viewed in the Packets List
- You can add many columns, some of which you may not have realized were available options



Configuring Preferences

		Cumulative Bytes	Ξ
	eld type	Custom	
	umber	DCE/RPC call (cn_call_id / dg_seqnum)	
🔽 Time Ti	me (fori	DCE/RPC context ID (cn_ctx_id)	
Source So	ource ad	Delta time	
Destination Destination	estinatio	Delta time (conversation)	
Protocol Pr	otocol	Delta time displayed	
Length Pa	acket ler	Dest addr (resolved)	
V Info Inf	formatio		
New Column Al	bsolute (Dest port (resolved)	
		Dest port (unresolved)	
		Destination address	
		Destination port	
		Expert Info Severity	
		FW-1 monitor if/direction	
		Fibre Channel OXID	
		Fibre Channel RXID	
		Frame Relay DLCI	
		Frequency/Channel	
		GPRS BSSGP TLLI	
		HP-UX Device ID	
		HP-UX Subsystem	
Properties		Hardware dest addr	-
Add Field type:		Absolute date and time	-



Questions?

Copyright © www.ine.com All rights reserved.