(WIRE)SHARK-FV or,

My
Favorite
Wireshark
Customizations

EDDIE FORERO

COMMUNICAONE Inc.
ACMX #365, CWNE #160

@HeyEddie on the Twitters

Doing the Blog thing at:
BadFi.com
CommunicaONE.com/blog

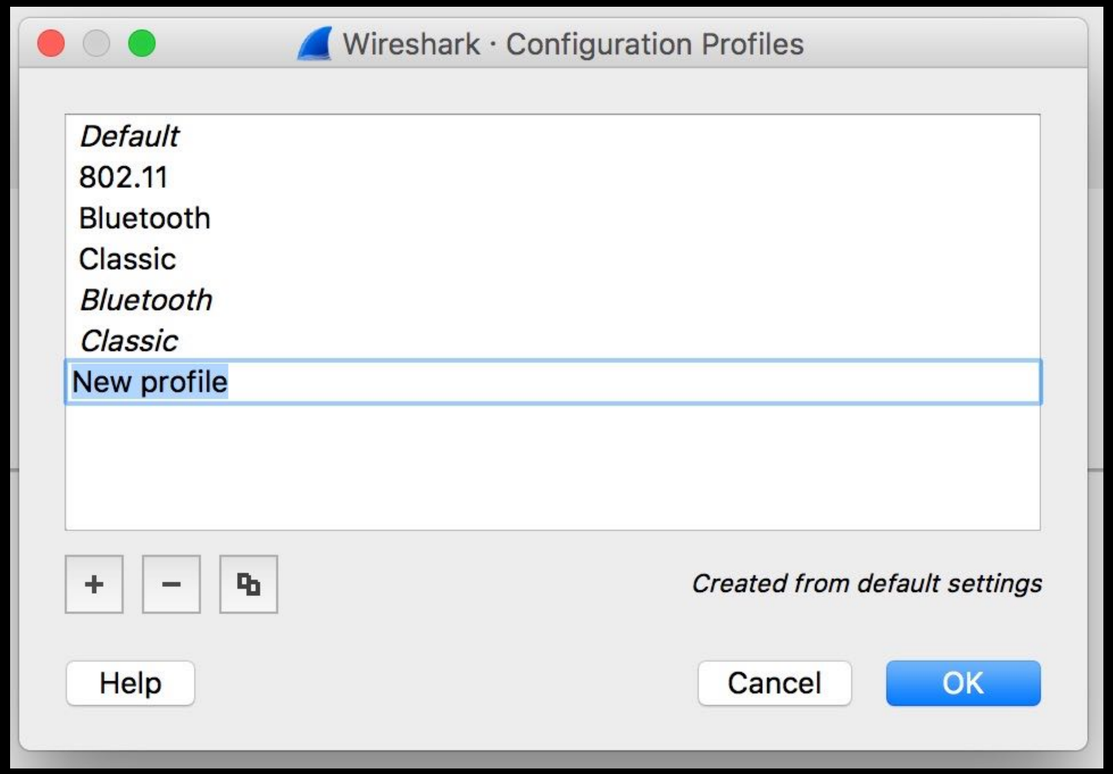
First Thing's First

- ***Native*** *support for RF Monitor mode*
- *Requires 3rd party software* ***Wireshark, Airtool,*** *etc.*
- *Hardware:* ***Internal NIC****,* ***Sidekick****, and now* ***WLAN PI****!*
- *Only option for* ***multi-channel*** *capture is Ekahau Sidekick (up to two channels)*

- *No* ***Native*** *support for RF Monitor mode*
- ***Requires*** *3rd Party software like* ***Wireshark****,* ***Omnipeek****,* ***Commview*** *for WiFI, etc.*
- *REQUIRES hardware like* ***Netgear A6210****,* ***Sidekick****, and now* ***WLAN PI!***
- *It'$ gonna* ***co$t*** *you $omething*
- *There are options available for* ***multi-channel*** *capture*
- ***OTHER OPTIONS:*** *https://badfi.com/blog/2018/6/14/options-for-wireless-packet-capture-in-windows*

#1 Custom Profiles

- *Preset profiles with your **favorite** settings*
- *Have Wireshark **ready to go** for the specific task at hand*
- *See **just what you want** to see*



#2 Columns that MATTER

No.	Time	Delta	Length	SA	DA	PHY type	Frame	Retry	RSSI	Duration	Size	Priority	Rate	MCS	SS	Ch.	Duration	SSID
500	0.000147	0.000147	371	ArubaNet_a1:1e:b4	Broadcast	802.11a	Beacon		-81 dBm	0	170358		12.0			36	232µs	COFE
501	0.008024	0.008024	403	Technico_cb:2f:2f	Broadcast	802.11a	Beacon		-86 dBm	0	170761		6.0			36	488µs	VirusServer-5G
506	0.043049	0.043049	355	ArubaNet_e0:2c:b1	Broadcast	802.11a	Beacon		-64 dBm	0	173867		6.0			36	424µs	b7c8238106940fd5b5174c83
507	0.000006	0.000006	304	ArubaNet_e0:2c:b2	Broadcast	802.11a	Beacon		-64 dBm	0	174171		12.0			36	188µs	COFE-Guest
508	0.000408	0.000408	368	ArubaNet_e0:2c:b3	Broadcast	802.11a	Beacon		-64 dBm	0	174539		12.0			36	232µs	COFE-Devices
509	0.000350	0.000350	360	AP-224	Broadcast	802.11a	Beacon		-64 dBm	0	174899		12.0			36	228µs	COFE
518	0.011648	0.011648	355	ArubaNet_a1:1e:b1	Broadcast	802.11a	Beacon		-82 dBm	0	177670		6.0			36	424µs	b7c8238106940fd5b5174c83
519	0.000005	0.000005	303	ArubaNet_a1:1e:b2	Broadcast	802.11a	Beacon		-81 dBm	0	177973		12.0			36	188µs	COFE-Guest
520	0.000393	0.000393	379	ArubaNet_a1:1e:b3	Broadcast	802.11a	Beacon		-81 dBm	0	178352		12.0			36	240µs	COFE-Devices
521	0.000284	0.000284	371	ArubaNet_a1:1e:b4	Broadcast	802.11a	Beacon		-81 dBm	0	178723		12.0			36	232µs	COFE
526	0.026111	0.026111	355	ArubaNet_e0:2c:b1	Broadcast	802.11a	Beacon		-64 dBm	0	181829		6.0			36	424µs	b7c8238106940fd5b5174c83
527	0.000006	0.000006	304	ArubaNet_e0:2c:b2	Broadcast	802.11a	Beacon		-64 dBm	0	182133		12.0			36	188µs	COFE-Guest
528	0.000105	0.000105	368	ArubaNet_e0:2c:b3	Broadcast	802.11a	Beacon		-64 dBm	0	182501		12.0			36	232µs	COFE-Devices
529	0.000473	0.000473	360	AP-224	Broadcast	802.11a	Beacon		-64 dBm	0	182861		12.0			36	228µs	COFE
530	0.027634	0.027634	355	ArubaNet_a1:1e:b1	Broadcast	802.11a	Beacon		-81 dBm	0	183216		6.0			36	424µs	b7c8238106940fd5b5174c83
531	0.000002	0.000002	303	ArubaNet_a1:1e:b2	Broadcast	802.11a	Beacon		-82 dBm	0	183519		12.0			36	188µs	COFE-Guest

- ***Know*** *what your looking at*
- ***Choose*** *the columns you want to see*
- ***Create*** *your own columns*

#3 Colorizing Packets (frames) ¯_(ツ)_/¯

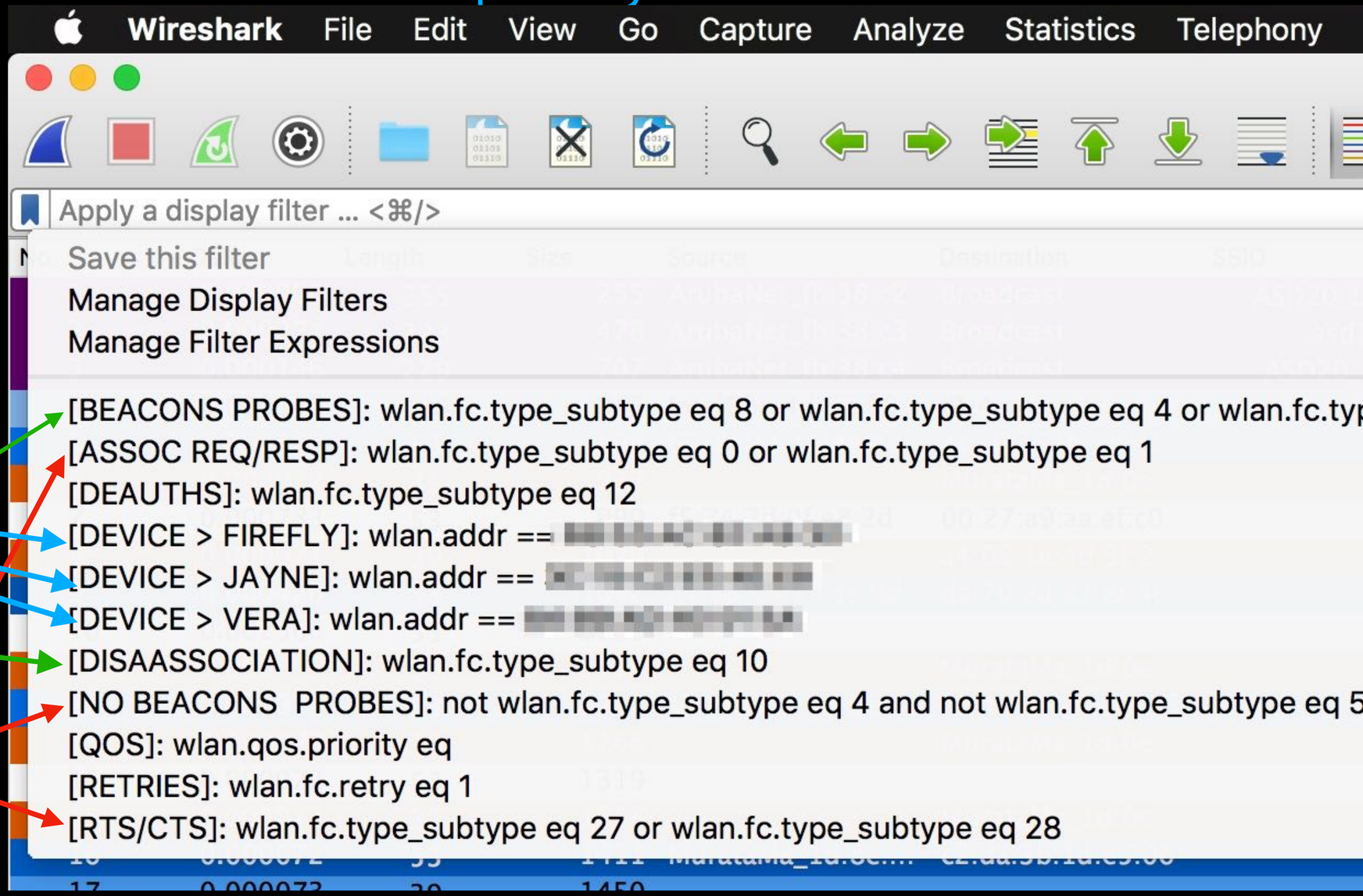
SA	DA	Frame	Retry	RSSI	Duration	Size	Priority	Rate
IntelCor_d4:df:c8	ZebraTec_91:8d:90	QOS Null		-53 dBm	60	84	Best Effort (Best Effort)	6.0
WistronN_ee:b1:6b	Broadcast	ProbeREQ		-53 dBm	0	186		2.0
SamsungE_11:c1:68	ZebraTec_91:8d:90	Null		-55 dBm	44	270		24.0
	IntelCor_4c:a1:6c (74:70:fd:4c:a1:6c) (RA)	ACK		-70 dBm	0	338		6.0
ZebraTec_95:d8:80 (84:24:8d:95:d8:80) (TA)	IntelCor_f0:63:3d (b8:8a:60:f0:63:3d) (RA)	BlockACK		-68 dBm	0	426		24.0
ZebraTec_95:d8:80	Broadcast	Beacon		-70 dBm	0	761		24.0
	ZebraTec_95:d8:80 (84:24:8d:95:d8:80) (RA)	CTS		-72 dBm	114	829		24.0
ZebraTec_95:d8:80 (84:24:8d:95:d8:80) (TA)	IntelCor_f0:63:3d (b8:8a:60:f0:63:3d) (RA)	RTS		-69 dBm	966	905		24.0

- ***Know*** *what your looking at*
- *Based on* ***Metageek Eye P.A.*** *color scheme*
- ***Customize*** *your own color palette*
- *Install* ***pre-configured*** *color palettes*

Download over ***there*** 👉 *https://support.metageek.com/hc/en-us/articles/115013527388*

#4 Custom Display Filters

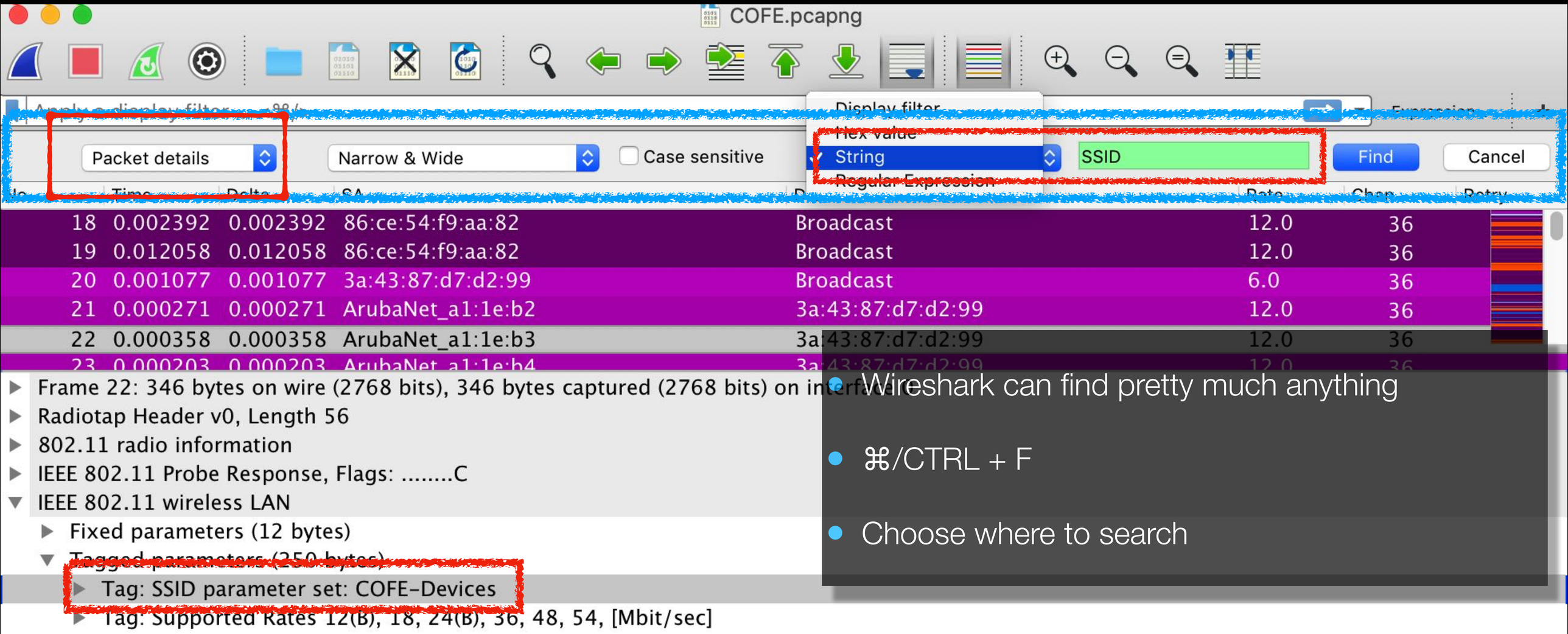
- *Clients*
- *Frame types*
- *Group filters together*



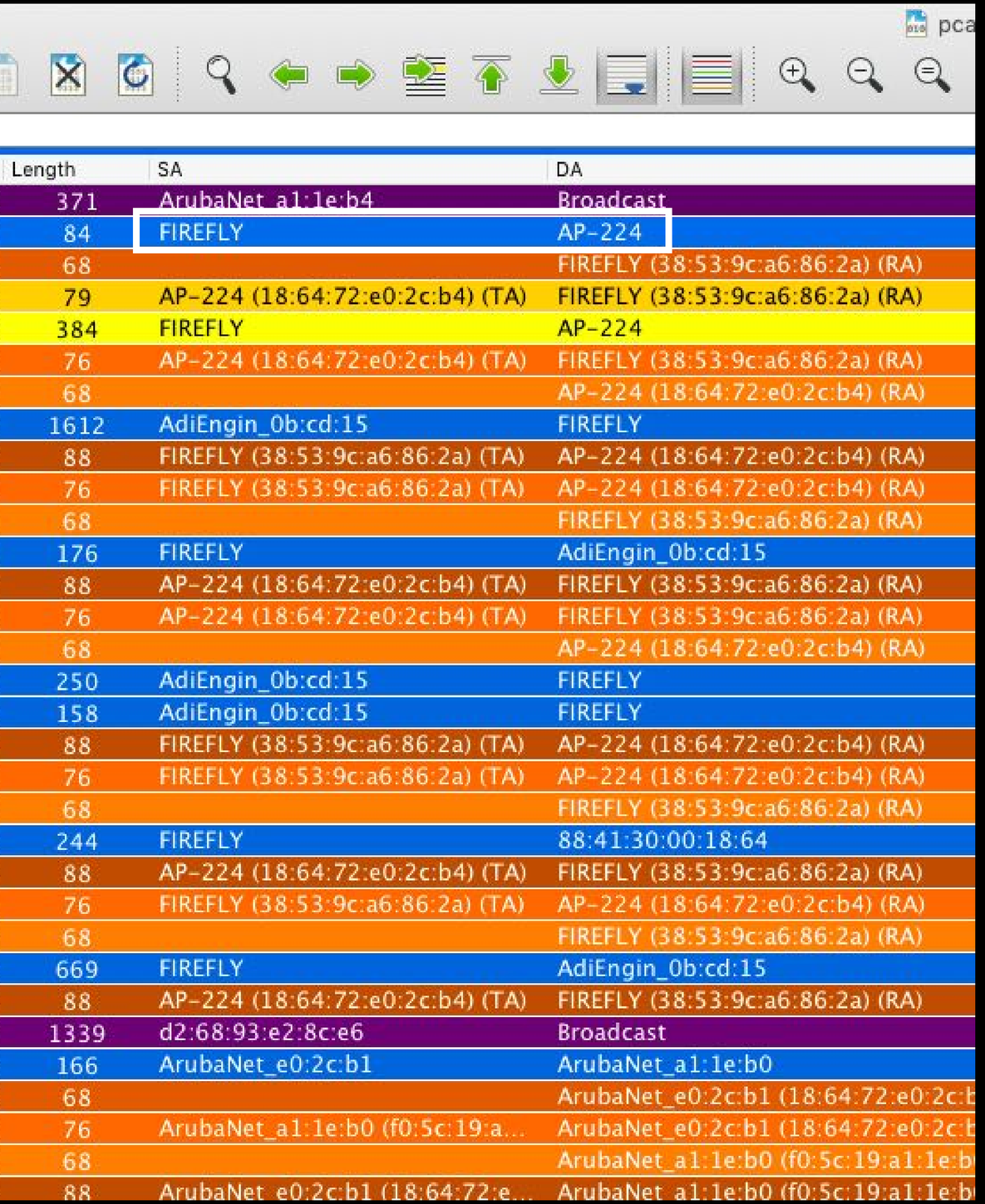
Wireshark · Display Filter Reference: IEEE 802.11 wireless LAN: https://www.wireshark.org/docs/dfref/w/wlan.html

#5 Search for Stuff

Make FIND Fun Again!



- Wireshark can find pretty much anything
- ⌘/CTRL + F
- Choose where to search



Length	SA	DA
371	ArubaNet_a1:1e:b4	Broadcast
84	FIREFLY	AP-224
68		FIREFLY (38:53:9c:a6:86:2a) (RA)
79	AP-224 (18:64:72:e0:2c:b4) (TA)	FIREFLY (38:53:9c:a6:86:2a) (RA)
384	FIREFLY	AP-224
76	AP-224 (18:64:72:e0:2c:b4) (TA)	FIREFLY (38:53:9c:a6:86:2a) (RA)
68		AP-224 (18:64:72:e0:2c:b4) (RA)
1612	AdiEngin_0b:cd:15	FIREFLY
88	FIREFLY (38:53:9c:a6:86:2a) (TA)	AP-224 (18:64:72:e0:2c:b4) (RA)
76	FIREFLY (38:53:9c:a6:86:2a) (TA)	AP-224 (18:64:72:e0:2c:b4) (RA)
68		FIREFLY (38:53:9c:a6:86:2a) (RA)
176	FIREFLY	AdiEngin_0b:cd:15
88	AP-224 (18:64:72:e0:2c:b4) (TA)	FIREFLY (38:53:9c:a6:86:2a) (RA)
76	AP-224 (18:64:72:e0:2c:b4) (TA)	FIREFLY (38:53:9c:a6:86:2a) (RA)
68		AP-224 (18:64:72:e0:2c:b4) (RA)
250	AdiEngin_0b:cd:15	FIREFLY
158	AdiEngin_0b:cd:15	FIREFLY
88	FIREFLY (38:53:9c:a6:86:2a) (TA)	AP-224 (18:64:72:e0:2c:b4) (RA)
76	FIREFLY (38:53:9c:a6:86:2a) (TA)	AP-224 (18:64:72:e0:2c:b4) (RA)
68		FIREFLY (38:53:9c:a6:86:2a) (RA)
244	FIREFLY	88:41:30:00:18:64
88	AP-224 (18:64:72:e0:2c:b4) (TA)	FIREFLY (38:53:9c:a6:86:2a) (RA)
76	FIREFLY (38:53:9c:a6:86:2a) (TA)	AP-224 (18:64:72:e0:2c:b4) (RA)
68		FIREFLY (38:53:9c:a6:86:2a) (RA)
669	FIREFLY	AdiEngin_0b:cd:15
88	AP-224 (18:64:72:e0:2c:b4) (TA)	FIREFLY (38:53:9c:a6:86:2a) (RA)
1339	d2:68:93:e2:8c:e6	Broadcast
166	ArubaNet_e0:2c:b1	ArubaNet_a1:1e:b0
68		ArubaNet_e0:2c:b1 (18:64:72:e0:2c:b
76	ArubaNet_a1:1e:b0 (f0:5c:19:a...	ArubaNet_e0:2c:b1 (18:64:72:e0:2c:b
68		ArubaNet_a1:1e:b0 (f0:5c:19:a1:1e:b
88	ArubaNet_e0:2c:b1 (18:64:72:e...	ArubaNet_a1:1e:b0 (f0:5c:19:a1:1e:b

#6

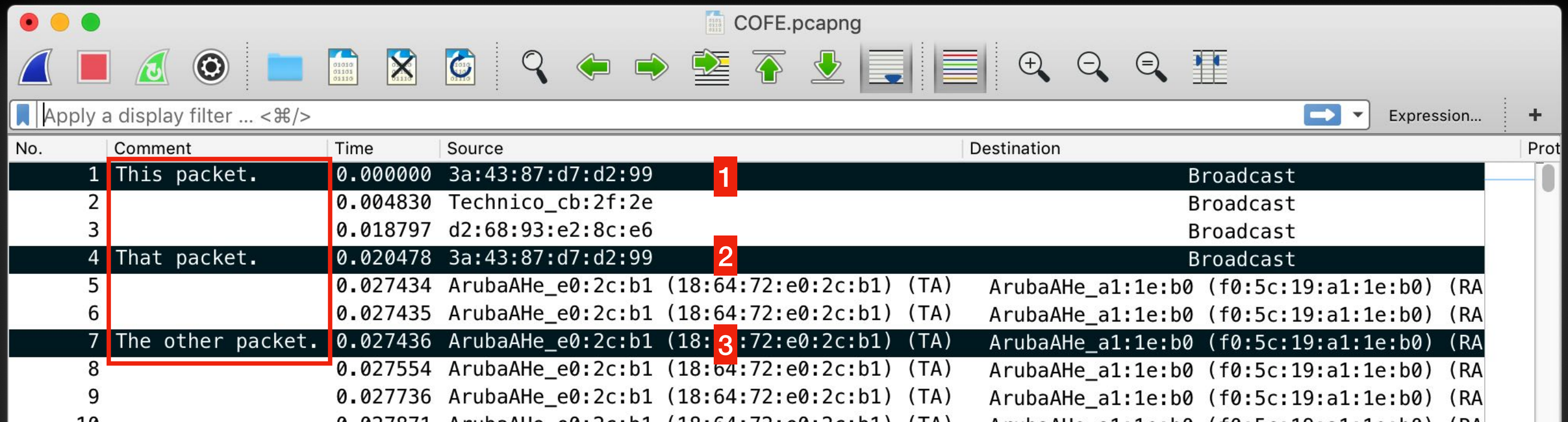
Custom Name Resolution

- *Name your **clients** for easy viewing*
- *Name your **APs** so you know it's the right one*
- *It's just plain **convenient***

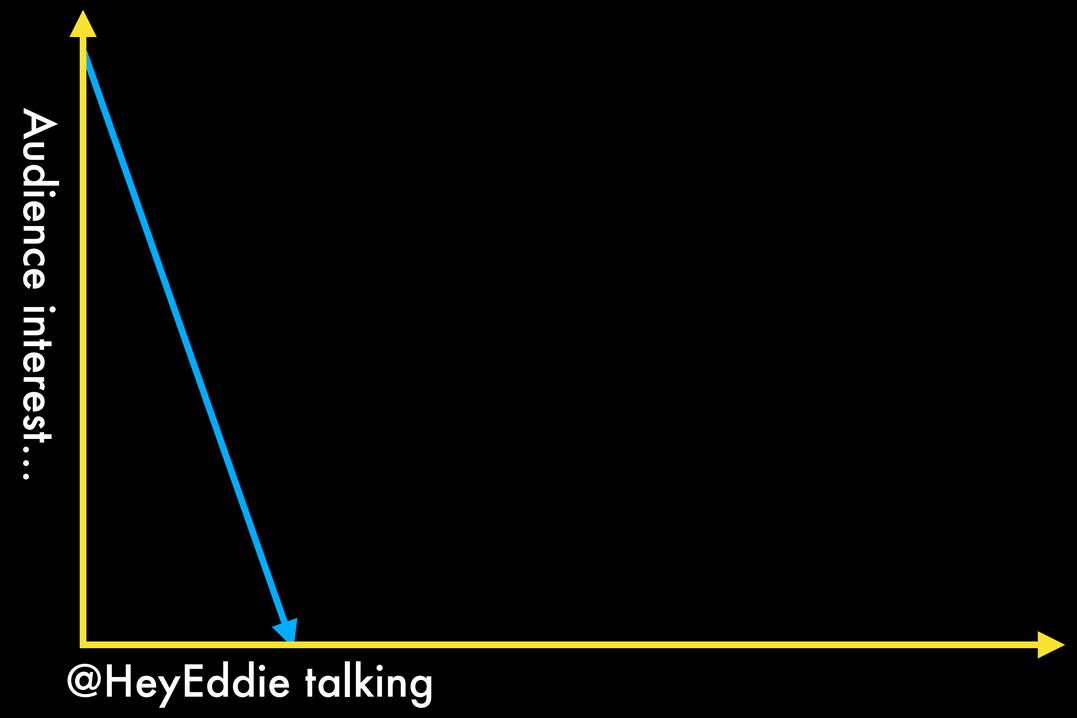
#7 Save that Frame!

(Selecting, exporting, & commenting on frames/packets.)

- Save only the frames you want
- Comment of specific frames (only supported in .pcapng format)
- Save for studying, later review, teaching, walking customer through flow, etc.



#8 Graph ALL THE THINGS!



- Get a **quick** overview
- Filter for only frames that **matter**

Helpful **Links**

Airtool by @AdrianGranados
https://www.adriangranados.com/apps/airtool

CWAP Certified Wireless Analysis Professional Official Study Guide (PW0-270)
https://www.amazon.com/Certified-Wireless-Analysis-Professional-Official-dp-0470769033/dp/0470769033/ref=mt_paperback?_encoding=UTF8&me=&qid=1550449598

Options for Wireless Packet Capture in Windows
https://badfi.com/blog/2018/6/14/options-for-wireless-packet-capture-in-windows

Wireshark · Display Filter Reference: IEEE 802.11 wireless LAN
https://www.wireshark.org/docs/dfref/w/wlan.html

Wireshark Color Profile – MetaGeek Support
https://support.metageek.com/hc/en-us/articles/115013527388

Wireshark for Wireless LANs LiveLessons by Jerome Henry (@WirelessCCIE) **& James Garringer** (@JamesGarringer)
http://www.informit.com/store/wireshark-for-wireless-lans-livelessons-9780134767536

WLAN PI
https://www.wlanpi.com