



WizShark™

WiFi Troubleshooting Made Easy

Gopinath KN
VP, Engineering

Robert Ferruolo
Sr. Technical Marketing Engineer

@WizShark, @gopinathkn, @raferruolo

CWNP - 2014

Motivation



This is how the Wi-Fi Troubleshooting world appears without Wizshark ...

A Typical Wi-Fi Connectivity Issue

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

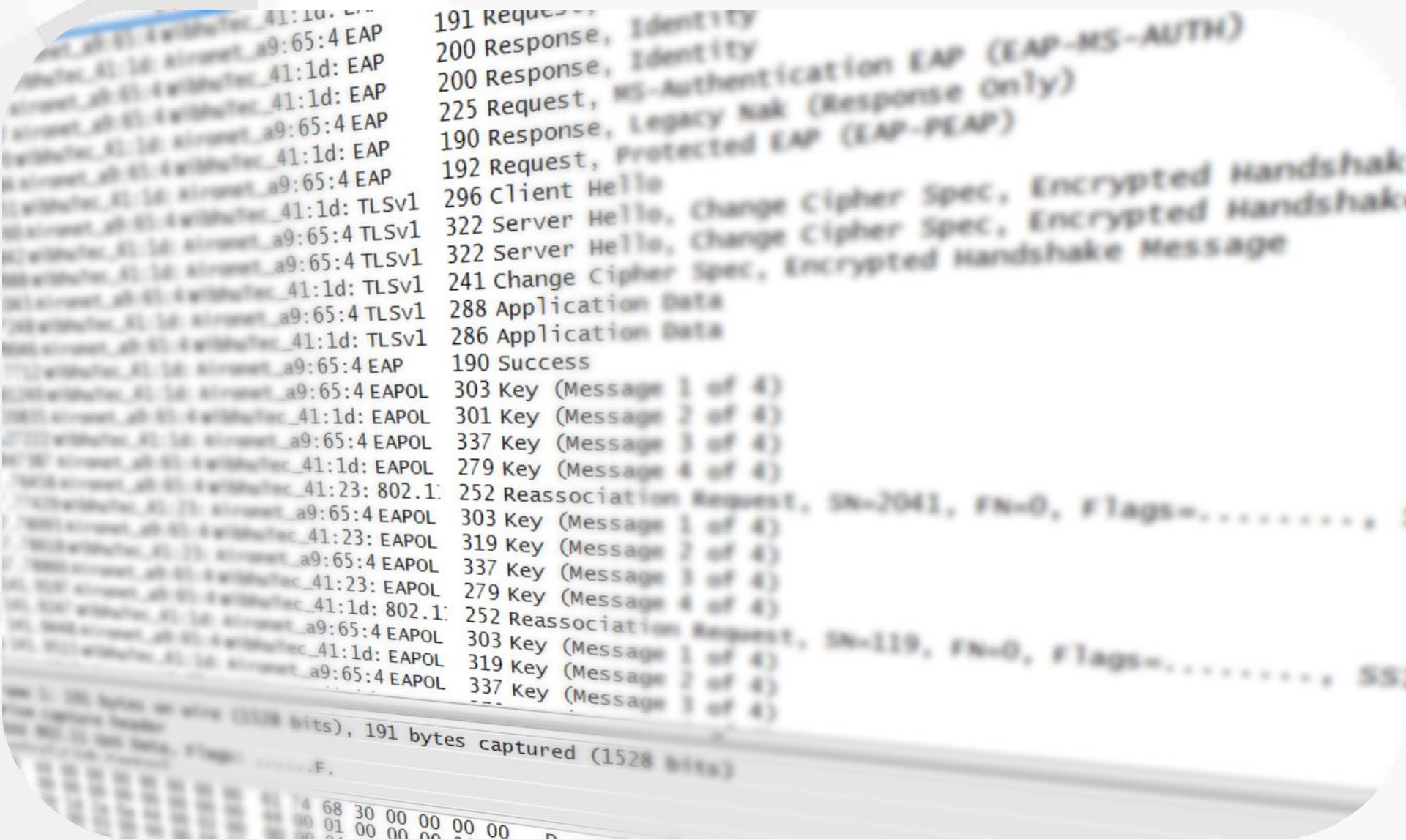
Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	wibhuTec_41:1d	Aironet_a9:65:4	EAP	191	Request, Identity
2	0.023687	Aironet_a9:65:4	wibhuTec_41:1d	EAPOL	185	Start
3	0.027557	wibhuTec_41:1d	Aironet_a9:65:4	EAP	191	Request, Identity
4	0.037912	Aironet_a9:65:4	wibhuTec_41:1d	EAP	200	Response, Identity
5	0.119497	Aironet_a9:65:4	wibhuTec_41:1d	EAP	200	Response, Identity
6	3.220720	wibhuTec_41:1d	Aironet_a9:65:4	EAP	225	Request, MS-Authentication EAP (EAP-MS-AUTH)
7	3.230084	Aironet_a9:65:4	wibhuTec_41:1d	EAP	190	Response, Legacy Nak (Response Only)
8	3.240651	wibhuTec_41:1d	Aironet_a9:65:4	EAP	192	Request, Protected EAP (EAP-PEAP)
9	3.265360	Aironet_a9:65:4	wibhuTec_41:1d	TLSv1	296	Client Hello
10	3.282842	wibhuTec_41:1d	Aironet_a9:65:4	TLSv1	322	Server Hello, Change Cipher Spec, Encrypted Handshake Message
11	3.282988	wibhuTec_41:1d	Aironet_a9:65:4	TLSv1	322	Server Hello, Change Cipher Spec, Encrypted Handshake Message
12	3.301043	Aironet_a9:65:4	wibhuTec_41:1d	TLSv1	241	Change Cipher Spec, Encrypted Handshake Message
13	3.317248	wibhuTec_41:1d	Aironet_a9:65:4	TLSv1	288	Application Data
14	3.359046	Aironet_a9:65:4	wibhuTec_41:1d	TLSv1	286	Application Data
15	3.377712	wibhuTec_41:1d	Aironet_a9:65:4	EAP	190	Success
16	3.381240	wibhuTec_41:1d	Aironet_a9:65:4	EAPOL	303	Key (Message 1 of 4)
17	3.420835	Aironet_a9:65:4	wibhuTec_41:1d	EAPOL	301	Key (Message 2 of 4)
18	3.427222	wibhuTec_41:1d	Aironet_a9:65:4	EAPOL	337	Key (Message 3 of 4)
19	3.447387	Aironet_a9:65:4	wibhuTec_41:1d	EAPOL	279	Key (Message 4 of 4)
20	67.76458	Aironet_a9:65:4	wibhuTec_41:23: 802.1	802.11	252	Reassociation Request, SN=2041, FN=0, Flags=....., SSID=OKC_TEST1
21	67.77429	wibhuTec_41:23:	Aironet_a9:65:4	EAPOL	303	Key (Message 1 of 4)
22	67.78093	Aironet_a9:65:4	wibhuTec_41:23:	EAPOL	319	Key (Message 2 of 4)
23	67.78618	wibhuTec_41:23:	Aironet_a9:65:4	EAPOL	337	Key (Message 3 of 4)
24	67.78860	Aironet_a9:65:4	wibhuTec_41:23:	EAPOL	279	Key (Message 4 of 4)
25	141.9197	Aironet_a9:65:4	wibhuTec_41:1d: 802.1	802.11	252	Reassociation Request, SN=119, FN=0, Flags=....., SSID=OKC_TEST1[Malformed Packet]
26	141.9247	wibhuTec_41:1d:	Aironet_a9:65:4	EAPOL	303	Key (Message 1 of 4)

Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)

- Prism capture header
- IEEE 802.11 QoS Data, Flags:F.
- Logical-Link Control
- 802.1X Authentication

```
0000 44 00 00 00 90 00 00 00 61 74 68 30 00 00 00 00  D..... ath0....
0010 00 00 00 00 00 00 00 00 44 00 01 00 00 00 04 00  ..... D.....
0020 1b 1d 2a 0a 44 00 02 00 00 00 04 00 70 8f d2 c4  ..*.D... ..p...
0030 44 00 03 00 00 00 04 00 24 00 00 00 44 00 04 00  D..... $.D...
0040 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0050 00 00 00 00 44 00 06 00 00 00 04 00 3b 00 00 00  .....
n
```



```

41:1d: EAP
a9:65:4 EAP
41:1d: EAP
41:1d: EAP
a9:65:4 EAP
41:1d: EAP
a9:65:4 EAP
41:1d: TLSv1
a9:65:4 TLSv1
a9:65:4 TLSv1
41:1d: TLSv1
a9:65:4 TLSv1
41:1d: TLSv1
a9:65:4 EAP
a9:65:4 EAPOL
41:1d: EAPOL
a9:65:4 EAPOL
41:1d: EAPOL
a9:65:4 EAPOL
41:23: 802.1
a9:65:4 EAPOL
41:23: EAPOL
a9:65:4 EAPOL
41:23: EAPOL
41:1d: 802.1
a9:65:4 EAPOL
41:1d: EAPOL
a9:65:4 EAPOL
191 Request, Identity
200 Response, Identity
200 Response, Identity
225 Request, MS Authentication EAP (EAP-MS-AUTH)
190 Response, Legacy Nak (Response Only)
192 Request, Protected EAP (EAP-PEAP)
296 Client Hello
322 Server Hello, Change Cipher Spec, Encrypted Handshake Message
322 Server Hello, Change Cipher Spec, Encrypted Handshake Message
241 Change Cipher Spec, Encrypted Handshake Message
288 Application Data
286 Application Data
190 Success
303 Key (Message 1 of 4)
301 Key (Message 2 of 4)
337 Key (Message 1 of 4)
279 Key (Message 4 of 4)
252 Reassociation Request, SN=2041, FN=0, Flags=
303 Key (Message 1 of 4)
319 Key (Message 2 of 4)
337 Key (Message 1 of 4)
279 Key (Message 4 of 4)
252 Reassociation Request, SN=119, FN=0, Flags=
303 Key (Message 1 of 4)
319 Key (Message 2 of 4)
337 Key (Message 1 of 4)

```

1528 bits), 191 bytes captured (1528 bits)

```

..F.
4 68 30 00 00 00 00
90 01 00 00 00 00 00

```




Packet Trace Fatigue!

```
191 Request, Identity
200 Response, Identity
200 Response, Identity
225 Request, MS-Authentication EAP (EAP-MS-AUTH)
190 Response, Legacy Nak (Response only)
192 Request, Protected EAP (EAP-PEAP)
296 Client Hello
322 Server Hello, Change Cipher Spec, Encrypted Handshake
322 Server Hello, Change Cipher Spec, Encrypted Handshake
241 Change Cipher Spec, Encrypted Handshake Message
288 Application Data
286 Application Data
190 Success
303 Key (Message 1 of 4)
301 Key (Message 2 of 4)
337 Key (Message 1 of 4)
279 Key (Message 4 of 4)
252 Reassociation Request
303 Key (Message 1 of 4)
319 Key (Message 2 of 4)
337 Key (Message 1 of 4)
279 Key (Message 4 of 4)
252 Reassociation Request
303 Key (Message 1 of 4)
319 Key (Message 2 of 4)
337 Key (Message 1 of 4)
...
191 bytes captured (1528 bits)
```

Why the \$#!? Is Wi-Fi not working?





A Picture



is worth
=
=

Creamy, delicious, yummy,
fudge ice cream, smooth,
chocolate-chip mint ice
cream, strawberry ice
cream with real chunks of
strawberry, colored sugar
sprinkles, waffle sugar
cone, sweet, wonderful,
tastes great, cold, nice to
eat, dessert, good yummy
toppings, chocolate
sprinkles, comforting,
good, fun, dipping, terrific,

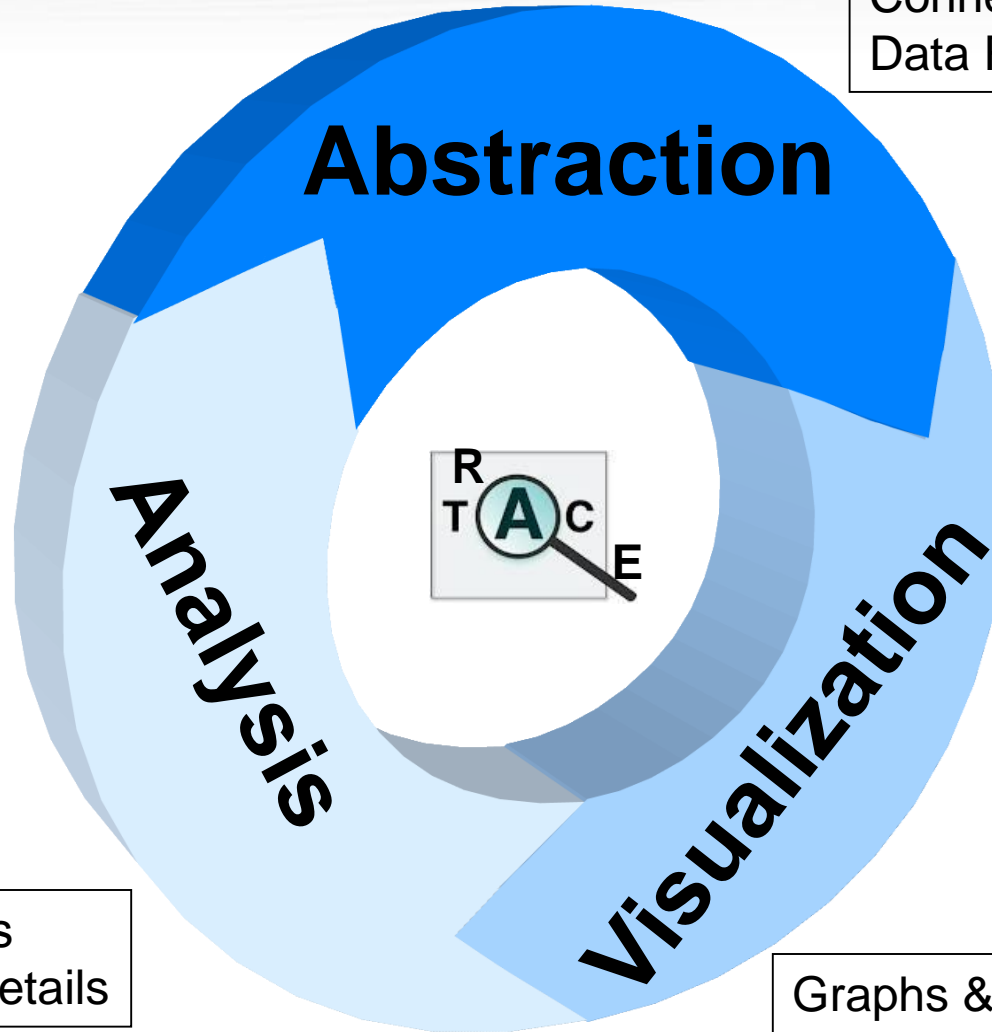
A thousand ~~words~~.

©2003 E. Aoyama

Packets

WizShark

Failure messages
Connection Handshake
Data Rates



“What-if” Scenarios
Packet Range & Details

Graphs & charts
Multiple views (AP & client)

Followed by vivek raval and 12 others

WizShark @WizShark · Aug 1
@KeithRParsons True. Objective is to help quickly identify part of traces that need frame analysis.

[View conversation](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

Retweeted by Gustavo Mastroianni

Keith R. Parsons @KeithRParsons · Jul 29
For those of you who asked... **Wizshark** does NOT remove the need for you to understand 802.11 frames and how they are supposed to interact.

[Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

Keith R. Parsons @KeithRParsons · Jul 29
Wizshark from @AirTight is a pretty cool way to do visual Wi-Fi analysis... check it out.
blog.airtightnetworks.com/wizshark-bring...

[Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

Andrew von Nagy @revolutionwifi · Jul 25
RT @CHemantC: @WizShark Brings Collaboration to #WiFi Troubleshooting shar.es/L3Q75 < Fresh ideas! Well done team! < +1 tools rock!

[Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

Lee Badman @wirednot · Jul 25
@CHemantC @WizShark WizShark is very nice. Great approach to analysis.

[Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)

Remember: We are NOT replacing the human brain or the need for knowledge

Providing better troubleshooting tools for making the process easy and enjoyable!



WizShark Demo

Key Takeaways

End-to-end remote troubleshooting from AirTight Cloud

Troubleshooting from a mobile device

Built-in trace sharing for collaboration

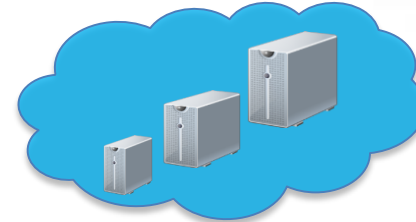
Wi-Fi vendor agnostic -- supports PCAP family



Value



Collaboration Tool



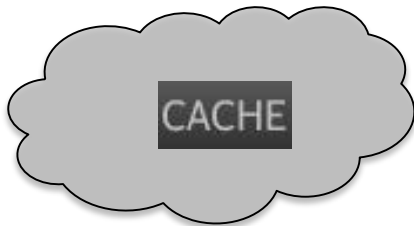
Scalability



Education Tool



Vendor Agnostic



Caching of Traces and Views



MSP Value Added Service





Questions

Comments

Suggestions



Thank You Wizshark Team

gopi@airtightnetworks.com
robert.ferruolo@airtightnetworks.com
Karan.gupta@airtightnetworks.com
Davneet.singh@airtightnetworks.com

wizshark@airtightnetworks.com