eye P.A.

visual packet analysis

metageek

Eye P.A. visual packet analysis

SYSTEM REQUIREMENTS

1) Microsoft .NET Framework 4 Client Profile (installer will direct you to download)
2) Microsoft .NET Framework 4 Extended (installer will direct you to download)
3) WinPcap (installer will direct you to download)

INSTALLATION

1) Download the latest version of Eye P.A. from MetaGeek
   http://www.metageek.net/products/eye-pa/download

2) Once the file has finished downloading, double-click on the installer. Go through the installation dialogue. The program will install under the directory "MetaGeek."

3) Double click on the icon "Eye P.A." to start the application.

   If this is the first time Eye P.A. is run, it will ask for a license key.

   If you do not have a license key, click on "Continue Trial" button to run Eye P.A. in evaluation mode for 15 days.

HOW TO GET A .pcap FILE

Eye P.A. is a wireless network data visualization tool. It sorts and displays data that has been captured in a .pcap file in order to make it easy for you to troubleshoot problems with your wireless network.

You can get a .pcap file in a lot of different ways. The ways listed below are the ones we're accustomed to gathering them with. We'd love to hear more about how you use .pcap files in our user fourm.

WITH **Windows and AirPcap Adapter**

AirPcap is a USB adapter that turns WireShark into a powerful 802.11 WLAN packet analysis tool for Windows computers. Use the AirPcap adapter to establish a baseline for every WLAN implementation and troubleshoot communication issues above and beyond the wired network. Select the adapter in WireShark and export the capture to a pcap file.

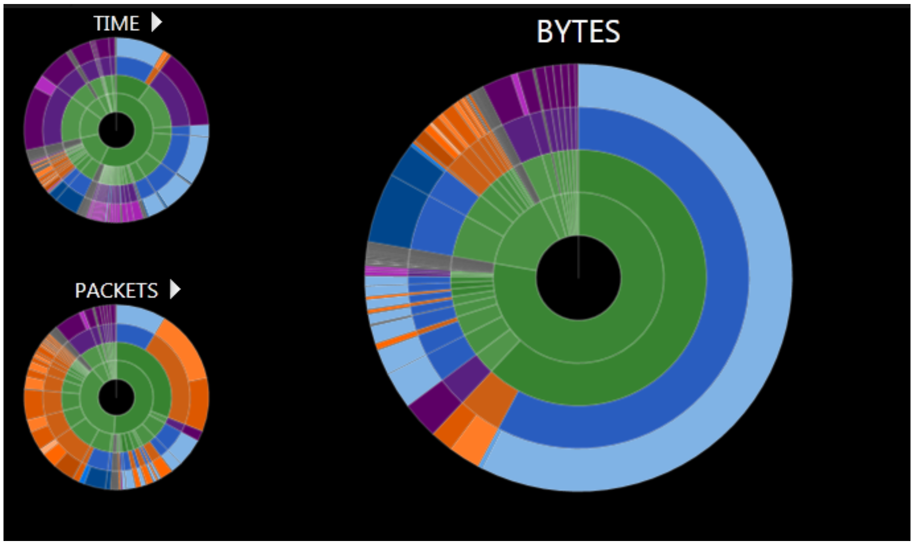
WITH **Mac OSX and WireShark**

Open the WireShark application to create a pcap file using the internal wireless network interface. Select the adapter en1 and click options to go into the advanced settings. Select "Capture packets in monitor mode" and then click start. WireShark will begin to log all of the wireless frames. Click file > save to create a .pcap which can be opened by Eye P.A.

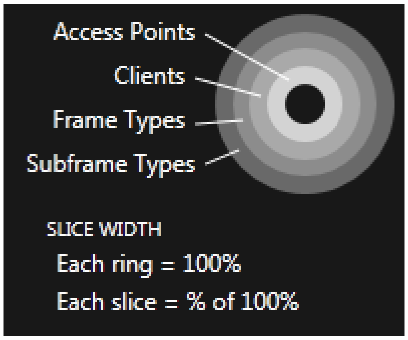
MAIN VIEWS

Multi-Layered Pie Charts

"Visually see wireless conversations between stations and access points."



Eye P.A. uses multi-layered pie charts to display overall utilization of total packets, total bytes and total amount of time. The size of the slices in the ring are proportionate to the total, while the colors represent the type of data being represented.

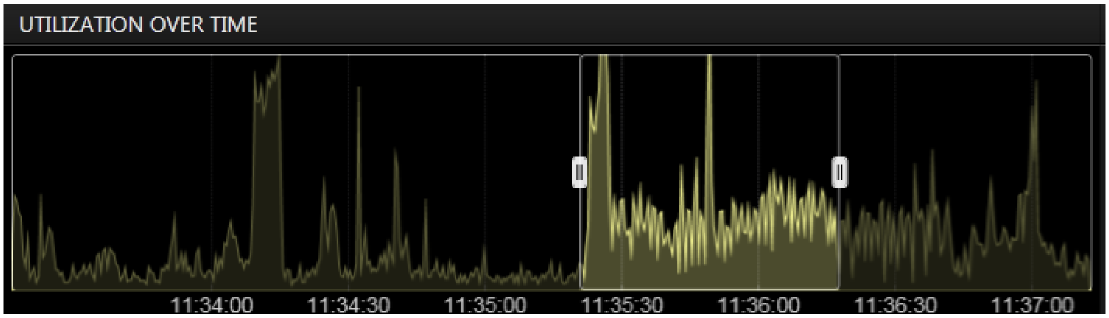


The data is a hierarchical breakdown by SSID > Client > Frame Type> Subframe Type. Each slice is divided into smaller slices in the next layer.

For example, by clicking on a client, Eye P.A. will draw a new multi-layered pie chart with all of the data for that particular client.

Time Graph

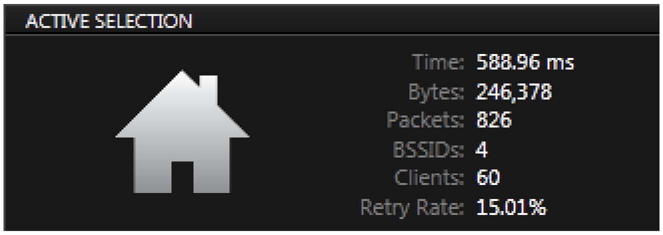
"Drill down to a smaller range of time to isolate the problem."



Eye P.A. displays a historical summary of the data capture in the bottom section. By default Eye P.A. displays the capture in its entirety. The user can change the window of time by dragging the start and stop handles. When the user selects a smaller time range both the data visuals and tables will update to only display data from the user's selected time range.

Active Selection Legend

“The active selection legend shows the most relevant statistics regarding the innermost center layer.”



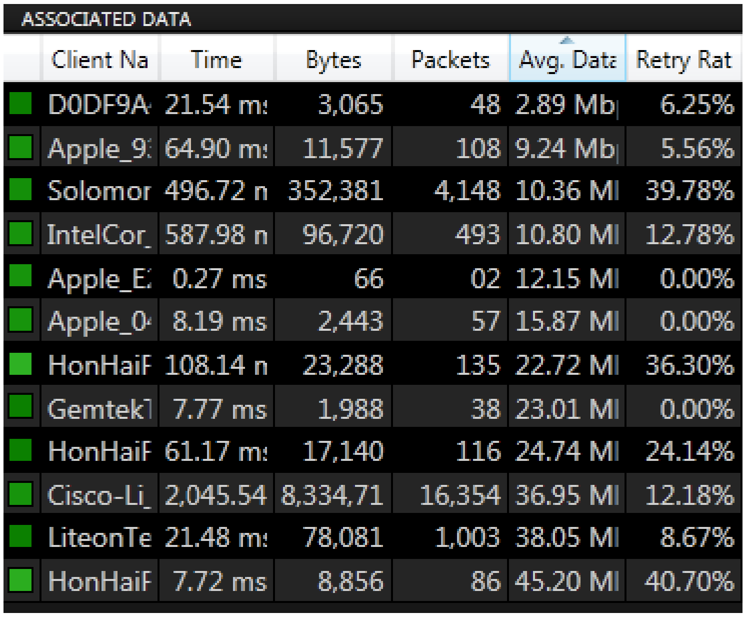
ACTIVE SELECTION

Time: 588.96 ms
Bytes: 246,378
Packets: 826
BSSIDs: 4
Clients: 60
Retry Rate: 15.01%

The active selection legend located in the top right represents the center. It will change as the user drills down through layers to display total time, bytes, data rate and other ring specific details.

Table

“The table in Eye P.A. brings out the metrics for each layer.”



ASSOCIATED DATA

	Client Na	Time	Bytes	Packets	Avg. Data	Retry Rat
🟩	D0DF9A	21.54 ms	3,065	48	2.89 Mb	6.25%
🟩	Apple_9	64.90 ms	11,577	108	9.24 Mb	5.56%
🟩	Solomor	496.72 n	352,381	4,148	10.36 Ml	39.78%
🟩	IntelCor_	587.98 n	96,720	493	10.80 Ml	12.78%
🟩	Apple_E	0.27 ms	66	02	12.15 Ml	0.00%
🟩	Apple_0	8.19 ms	2,443	57	15.87 Ml	0.00%
🟩	HonHaiF	108.14 n	23,288	135	22.72 Ml	36.30%
🟩	Gemtek	7.77 ms	1,988	38	23.01 Ml	0.00%
🟩	HonHaiF	61.17 ms	17,140	116	24.74 Ml	24.14%
🟩	Cisco-Li_	2,045.54	8,334,71	16,354	36.95 Ml	12.18%
🟩	LiteonTe	21.48 ms	78,081	1,003	38.05 Ml	8.67%
🟩	HonHaiF	7.72 ms	8,856	86	45.20 Ml	40.70%

The table displays quantifiable metrics for the layer succeeding the center (ring 1). Upon opening a pcap file the table will show each BSSID, the total amount of airtime utilized, bytes, number of clients associated, average data frame rate and retry rate.

Each column in the table can be clicked to sort from low to high or high to low. This will also rearrange the pie chart according to the ordering in the table.

MULTI-LAYERED PIE CHARTS

To alternate between the different visual types click the arrows above the pie charts on the left hand side. This will change the main pie chart and the time graph to that type.

Packets

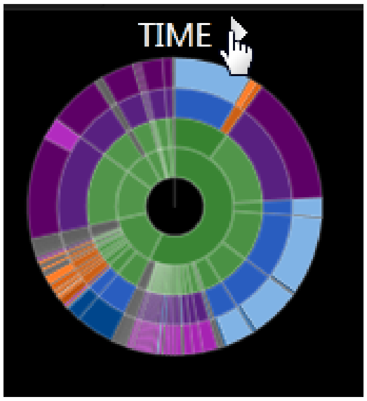
This multi-layer pie chart represents the proportionate amounts in comparison to the total packets captured.

Bytes

The pie chart represents 100% of the total data captured in Bytes. Each slice is the total data sent by BSSID or client.

Time

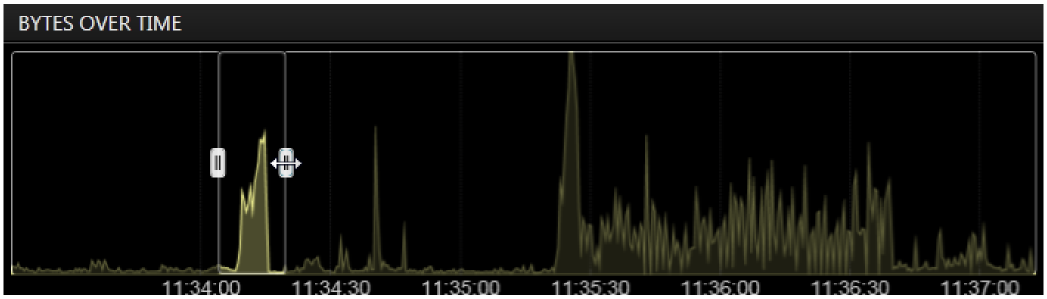
This pie chart displays the proportionate amount of air time each station utilized. It is important to note that lower data rates use more air time than higher data rates to transfer the same number of bytes.



RF communication is similar to a wired communication in the sense that no two devices can talk at the same time. Therefore the amount of time each station takes prohibits the other stations from transmitting.

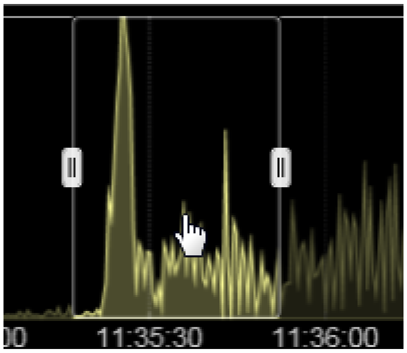
TIME GRAPH

Time Segment Analysis



Wireless environments can look different within minutes. Issues may be erratic and intermittent. By adjusting the time span the user can omit the times when the WLAN was functioning properly and focus on the small time window of when the issue occurred.

Adjusting Time Window



The time window is the line graph at the bottom of the window. When opening a pcap file in Eye P.A. the software will automatically adjust the time window to the start and end of the capture. The time window has two handles that can be adjusted inward and outward.

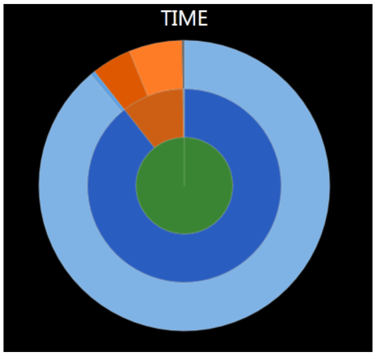
To move the time window click in the middle of the time window and drag it to another location in time.

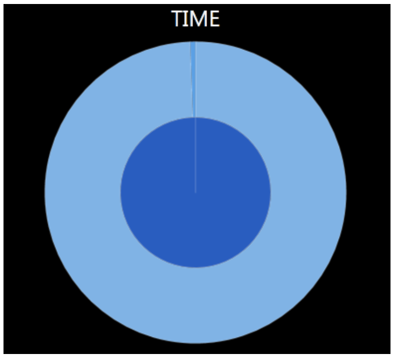
Packets, Bytes, and Time

The line graph represents the current largest multi-layered pie chart. The line chart will automatically change when the user toggles between the pie charts.

DATA VISUALS

Multi-Layered Pie Charts





There are 3 multi-layered pie charts in the main window. A multi-layered pie chart continually divides each slice into more slices. The size of the slice is proportionate to the total packets, bytes or time utilized.

Ring Order

The default ring order in Eye P.A. going in to outward.

1. BSSID
2. Associated Clients
3. Frame Type
4. Subframe Type

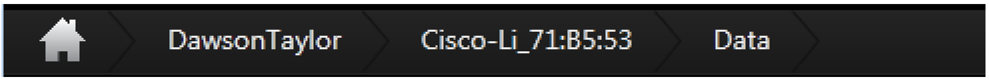
Drill-Down

Each element in the multi-layered pie chart can be clicked on to break it down even further into a new pie chart.

To return to a parent layer click the center of the pie chart. Or the home icon in the top left of the window.

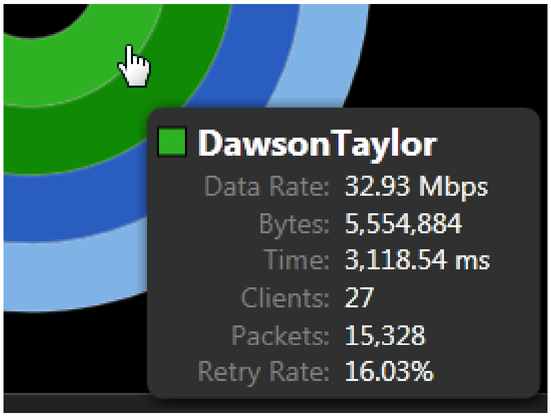
The layer directly outside of the center is represented in the table. Double clicking on a row will also drill down to that element as well.

Bread Crumbs



The bread crumbs represent the hierarchy of the current drill-down. Clicking home will return to the default view with no drill-downs applied. The bread crumbs represent each click the user made to get to the current pie chart. At any level, the user can click on a bread crumb to return to that mult-layered pie chart.

Hover (Inspector Tool)



🟩 DawsonTaylor
Data Rate: 32.93 Mbps
Bytes: 5,554,884
Time: 3,118.54 ms
Clients: 27
Packets: 15,328
Retry Rate: 16.03%

When a user hovers over a slice in the pie chart a box will appear and provide additional details like data rate, packet count and retry rate. This information is also displayed in the Associated Data Table.

UNDERSTANDING COLOR

Data Rate

The first two layers in the multi-layered pie chart are colored by the average data rate of the traffic. The shade of green is based on a sliding scale. The minimum average data rate captured is represented by a dark green while the highest is represented by a lighter green.

DATA RATE	COLOR
150+ Mbps	🟩
|	🟩
|	🟩
|	🟩
V	🟩
0 Mbps	🟩

Data Frames

Data frames carry the actual data passed down from higher layer protocols.

DATA PACKET TYPE	COLOR
QoS Data	🟦
QoS Data CF Poll	🟦
QoS Data CF Ack	🟦
QoS Data CF Ack CF Poll	🟦
QoS CF Ack CF Poll	🟦
QoS Null CF Ack CF Poll	🟦
QoS Null	🟦
Null Function No Data	🟦
CF Ack	🟦
CF Poll	🟦
CF Ack CF Poll	🟦
CF Ack No Data	🟦
CF Poll No Data	🟦
CF Ack CF Poll No Data	🟦
Data (Normal)	🟦

Management Frames

A majority of the frame types in an 802.11 network. Used by wireless stations to join and leave the network.

MANAGEMENT PACKET TYPE	COLOR
Disassocation	🟪
Deauthentication	🟪
Authentication	🟪
ATIM	🟪
Aruba	🟪
Probe Request	🟪
Probe Response	🟪
Association Request	🟪
Association Response	🟪
Reassociation Request	🟪
Reassociation Response	🟪
Reserved 0-3	🟪
Beacon	🟪

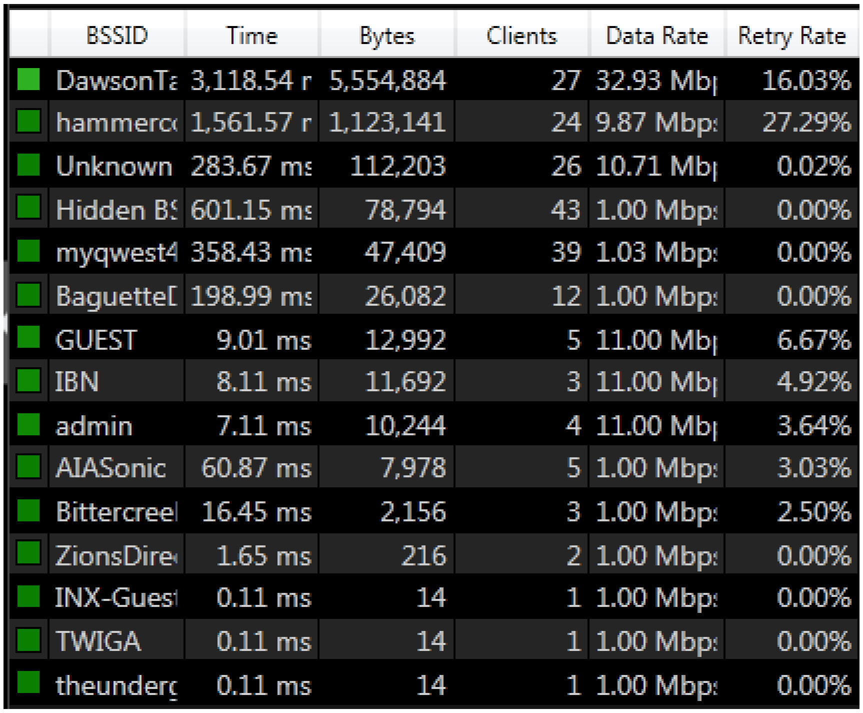
Control Frames

Control frames help deliver data frames by managing the access to the wireless medium.

Control frames help with the delivery of the data frames. Control frames must be able to be heard by all stations; therefore, they must be transmitted at one of the basic rates. Control frames are also used to clear the channel, acquire the channel, and provide unicast frame acknowledgments.

CONTROL PACKET TYPE	COLOR
PS Poll	🟧
CF End	🟧
CF End CF Ack	🟧
CTS	🟧
RTS	🟧
ACK	🟧
Block ACK	🟧
Block ACK REQ	🟧

ASSOCIATED DATA TABLE



	BSSID	Time	Bytes	Clients	Data Rate	Retry Rate
🟩	DawsonTa	3,118.54 r	5,554,884	27	32.93 Mb	16.03%
🟩	hammerc	1,561.57 r	1,123,141	24	9.87 Mbp	27.29%
🟩	Unknown	283.67 ms	112,203	26	10.71 Mb	0.02%
🟩	Hidden B	601.15 ms	78,794	43	1.00 Mbp	0.00%
🟩	myqwest4	358.43 ms	47,409	39	1.03 Mbp	0.00%
🟩	Baguette	198.99 ms	26,082	12	1.00 Mbp	0.00%
🟩	GUEST	9.01 ms	12,992	5	11.00 Mb	6.67%
🟩	IBN	8.11 ms	11,692	3	11.00 Mb	4.92%
🟩	admin	7.11 ms	10,244	4	11.00 Mb	3.64%
🟩	AIASonic	60.87 ms	7,978	5	1.00 Mbp	3.03%
🟩	Bittercree	16.45 ms	2,156	3	1.00 Mbp	2.50%
🟩	ZionsDire	1.65 ms	216	2	1.00 Mbp	0.00%
🟩	INX-Gues	0.11 ms	14	1	1.00 Mbp	0.00%
🟩	TWIGA	0.11 ms	14	1	1.00 Mbp	0.00%
🟩	theunder	0.11 ms	14	1	1.00 Mbp	0.00%

The Associated Data Table provides details for the innermost ring (Ring 1) of the Multi Layer Pie Chart.

Table Columns

- BSSID - This is the network name of the Access Point.
- MAC - A unique identifier for each network interface.
- Time - The amount of time used to transmit
- Bytes - The amount of data transferred
- Packets - The total # of packets per BSSID
- Retransmit - The percentage of packets that had to be resent.

LEARN MORE

You can learn more about Eye P.A. at our website
http://www.metageek.net/products/eye-pa