



1

2

3

WI-FI ROAMING ANALYSIS TOOLS HARDWARE / SOFTWARE REQUIREMENTS

1-2-3 with Globeron

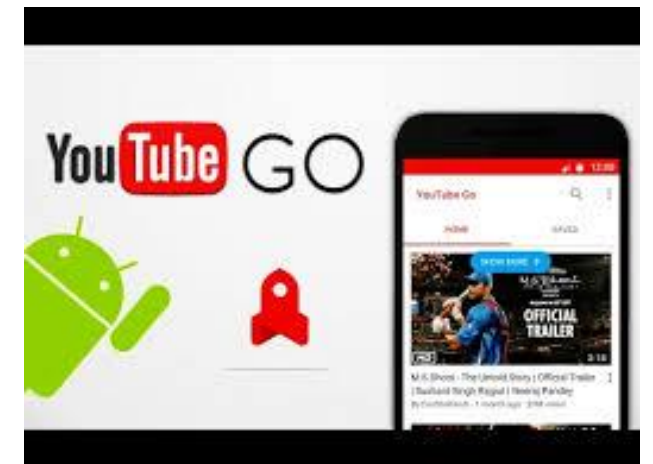


SCOPE — WI-FI ROAMING ANALYSIS & TOOLS

- The focus here is on the tools needed and vendors solutions available in the market to do proper roaming analysis at OSI Layer 1 (Physical Layer) using Spectrum Analyzers
- to do roaming analysis at OSI Layer 2 (Protocol Layer) at simultaneous channels (to capture clients roaming between different channels)

ROAMING - APPLICATIONS

- Normal roaming using data traffic either mobility (seamless roaming) or portability (it is allowed to lose connection in between APs, but it connects automatically)
- Voice over Wi-Fi communication (“Wi-Fi Calling”)
- Video over Wi-Fi communication or a combination of the solutions above



HARDWARE — OSI LAYER 1 - ANALYSIS

- Understand the 2.4 GHz and 5 GHz Spectrum by doing Spectrum Analysis
 - Learn to do signature analysis (recognize the different patterns of narrow-band and wide-band communication and signals)
 - Find non-Wi-Fi interfering sources and Wi-Fi interference (CCI, ACI)
 - Understand the difference between Swept-Tuned and Fast Fourier Transform Spectrum Analysis and how it impacts the spectrum analysis
-
- Make sure that your Wi-Fi network has a stable foundation.
 - Like these houses, you can walk “roam” easily to the neighbors...



STANDALONE SPECTRUM ANALYZERS AND OSCILLOSCOPES (NOT SO PORTABLE)



Front view of
the Sinewave



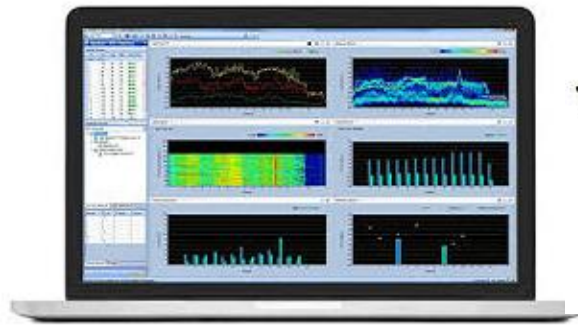
Side way view of
the Sinewave

HARDWARE — OSI LAYER 1 — LAPTOP BASED TOOLS

Portable - Spectrum Analyzers

- Netscout AirMagnet Spectrum XT + Spectrum XT USB Adapter
(includes signature analysis and signature recording and an alarm system of the type of interference) 2.4 GHz + 5 GHz
- Metageek Chanalyzer + Wi-Spy dBx adapter (2.4 GHz / 5 GHz), includes Spectral Masks overlap visualization and Wi-Fi mapping
- Cisco Spectrum Expert + PCMCIA Cardbus card (“Cognio Chipset”)
- Extreme AirDefense Mobile + PCMCIA Cardbus card (“Cisco or Netgear WAG511 card”)
- Ubiquiti AirView + USB dongle
- Smartphone / Tablet (Android or Apple iOS) + Oscium Pry 5x (2.4 GHz / 5 GHz)
- RF Explorer (handheld device) or connect to Android / iOS devices or Windows based systems
- Linux SpecAn tool + dBx adapter (2.4 GHz / 5 GHz), e.g. can run on a Odroid C2
- HackRF (Software Defined Radio – SDR) – Open source Spectrum Analyzer (fast Spectrum Analysis)

SPECTRUM ANALYZERS (2.4 GHz + 5 GHz)



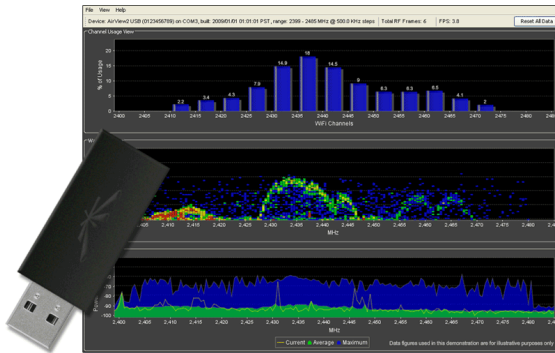
Netscout AirMagnet Spectrum XT + adapter



Metageek Chanalyzer + Wi-Spy DBx



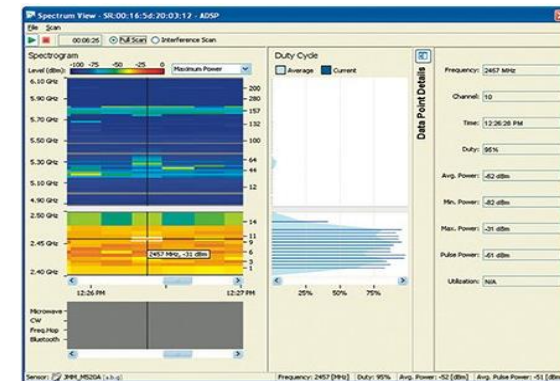
Cisco Spectrum Expert + PCMCIA (Cognio)



Ubiquiti AirView + adapter
(2.4 GHz only)

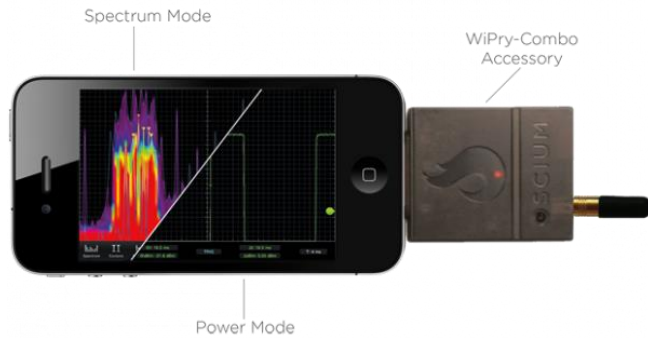


MacBook Pro + WiSpy (2.4 GHz only) + EaKiu



Extreme AirDefense Mobile

SPECTRUM ANALYZERS (2.4 GHZ + 5 GHZ)

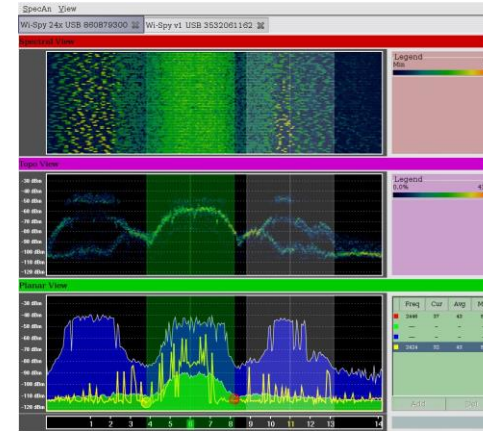


WiPry-Combo Accessory



(Singapore)

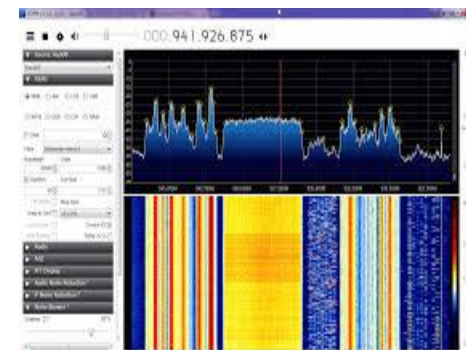
Oscium Wi-Pry 5x (dual band)



Linux – Kismet – SpecTools (SpecAn)+ WiSpy DBx
PC or Odroid / Raspberry Pi



RF Explorer 6G Combo (or RF Explorer Wi-Fi Combo)



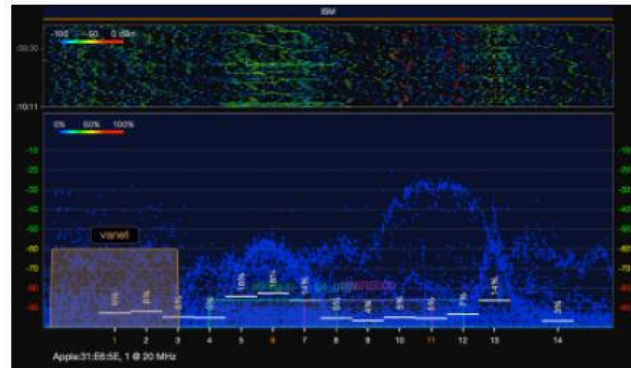
HackRF (RTL-SDR) "hackrf_sweep" on Linux / Windows / Android



SPECTRUM ANALYZERS (2.4 GHZ + 5 GHZ)



Apple MacBookPro OSX



WiFi Explorer

Do more than finding wireless networks

WiFi Explorer Pro's spectrum analysis integration lets you visualize RF information and correlate it with Wi-Fi data to identify non-802.11 energy sources and better understand the effects of interference and channel utilization on your wireless network. Compatible spectrum analyzers:

- MetaGeek's [Wi-Spy 2.4x \(Version 2\)](#) & [Wi-Spy DBx](#)
- [Ekahau Spectrum Analyzer](#)
- [RF Explorer Wi-Fi Combo](#)
- [UberTooth One](#)
- [HackRF One](#) (Experimental)



Any of these:

Metageek Wi-Spy dBx
(or Ekahau OEM)



RF Explorer Wi-Fi Combo
(and probably 6G Combo)



Hack-RF
measurement in dBFS and not dBm
conversion from dBFS to dBm requires
calibration and goes beyond my expertise.

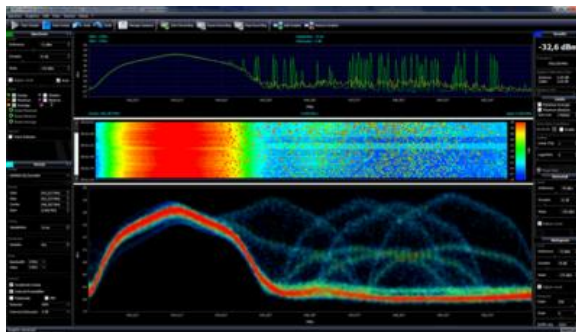


uberTooth One
(BlueTooth)

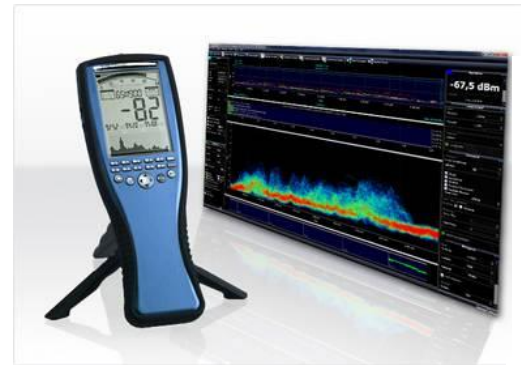
2.4 GHz

SPEKTRUMANALYSATOR SOFTWARE AARONIA MCS REQUIRES A SPECAN CAPTURE DEVICE

- <http://www.aaronia-shop.com/produkte/spectrum-analyzer>
- <http://spectran-developer.net/web/index.php?id=9>



Aaronia MCS



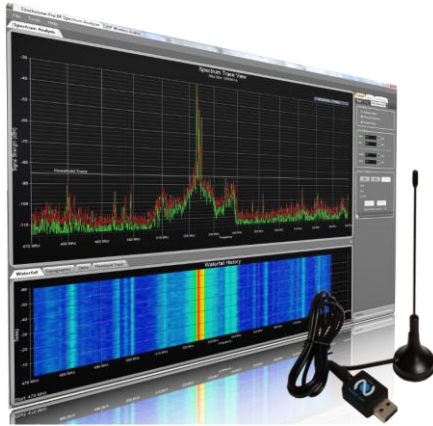
SpecAN devices



SPECTRAN HF V3: **Version 2.2**
SPECTRAN HF V4: **BETA 42**
SPECTRAN NF: **Version 1.0**



SPECTRUM ANALYZERS (2.4 GHZ + 5 GHZ)



Nuts about Nets – RF Viewer (WideBand)



Also other software:

Nuts about Nets – Clear Waves + RF Explorer

Nuts about Nets – Wi-Fi Surveyor

Nuts about Nets Touchstone + RF Explorer Wi-Fi or RF Explorer 6G Combo

Windows and Apple MAC OS X and Android (Smartphone/Tablet with USD-OTG “on-the-go” support)

INTERFERENCE DETECTION 2.4 GHZ / 5 GHZ (NOT A SPECTRUM ANALYZER, BUT DETECTS OSI-LAYER 1)

- AirHORN
- Baby Monitor
- Bluetooth Device
- Canopy Device
- Cordless Phone
- Game Controller (non-Bluetooth)
- Microwave Oven
- Motion Detector
- Narrowband RF Jammer
- Possible Interferer
- Radar

- Unclassified Interferer
- Video Monitor
- Wireless Bridge
- Wireless Mouse (non-Bluetooth)
- Wireless Video Camera
- ZigBee Device

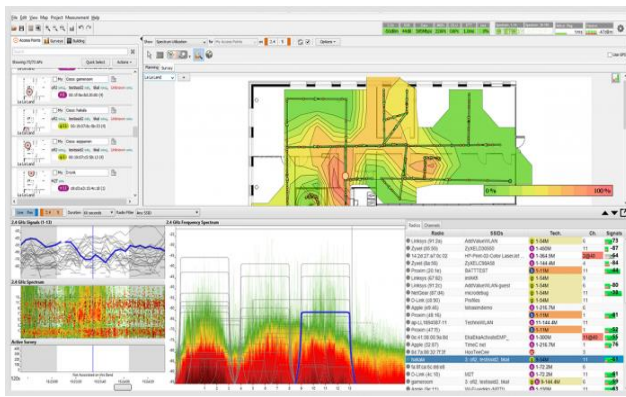


HARDWARE — OSI LAYER 1 — LAPTOP BASED TOOLS

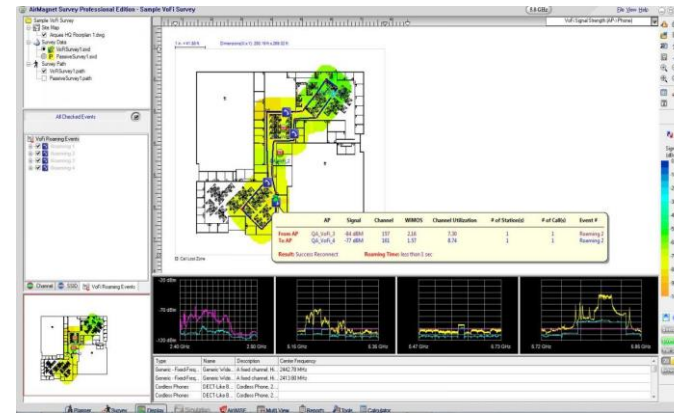
Integrated Spectrum Analysis with Site Survey Software

- Ekahau Site Survey + external “Sidekick” device (fast dual band Spectrum analysis)
- Ekahau Site Survey + Wi-Spy dBx adapter (multiple are supported to scan faster per RF band)
- Netscout AirMagnet Site Survey Pro + Spectrum XT + Spectrum XT USB Adapter
- Tamograph + Wi-Spy dBx adapter (multiple are supported to scan faster per RF band)
- Visiwave + Wi-Spy dBx adapter (Metageek Chanalyzer integration)

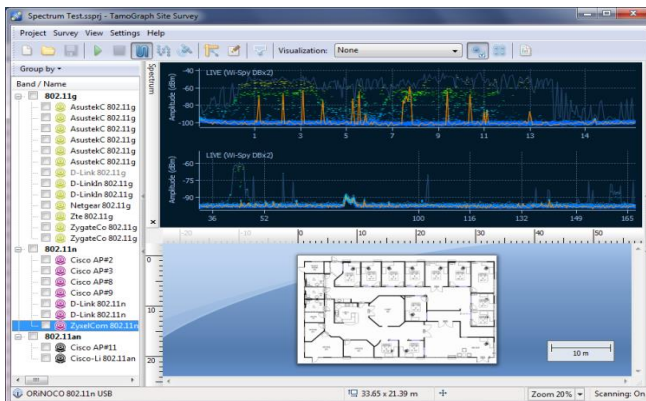
SPECTRUM ANALYZERS SITE SURVEY TOOLS + INTEGRATED SPECTRUM ANALYSIS



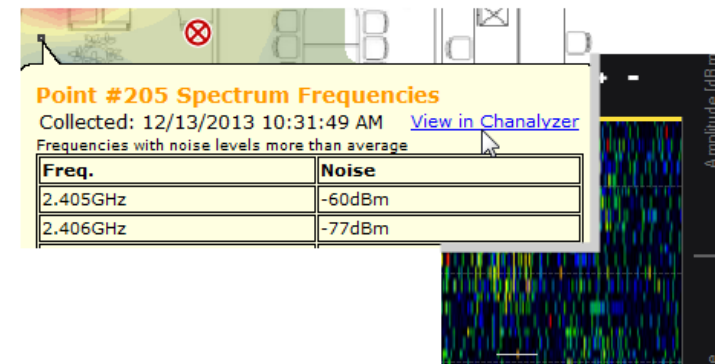
Ekahau Site Survey (ESS) + Wi-Spy adapter or Sidekick



Netscout AirMagnet Survey Pro + Spectrum XT adapter



Tamograph + Wi-Spy adapter



Visiwave + Wi-Spy adapter

HARDWARE — OSI LAYER 1 — AP BASED TOOLS

“RADIO SENSORS”

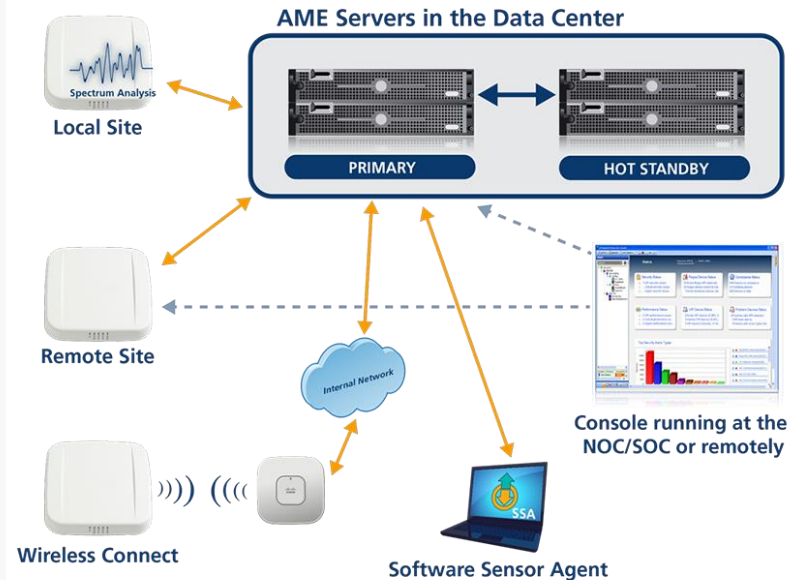
- **Access Point (AP) based Spectrum Analyzers**
also known as Radio Sensors or Radios in Sensor mode
- Cisco AP (Cognio Chipset / Clean Air)
- Cisco Meraki AP
- HPE / Aruba AP
- Aerohive AP
- Mojo Networks (aka AirTight Networks) AP
- Extreme Networks (aka Zebra Technologies / Motorola Solutions / AirDefense)
- Arris / Brocade / Ruckus Wireless APs
- Netscout AirMagnet Enterprise + Radio Sensors

SPECTRUM ANALYSIS USING AN AP/RADIO SENSOR

- Fixed setup – Remote Spectrum Analysis using APs in fixed locations in the office or global locations



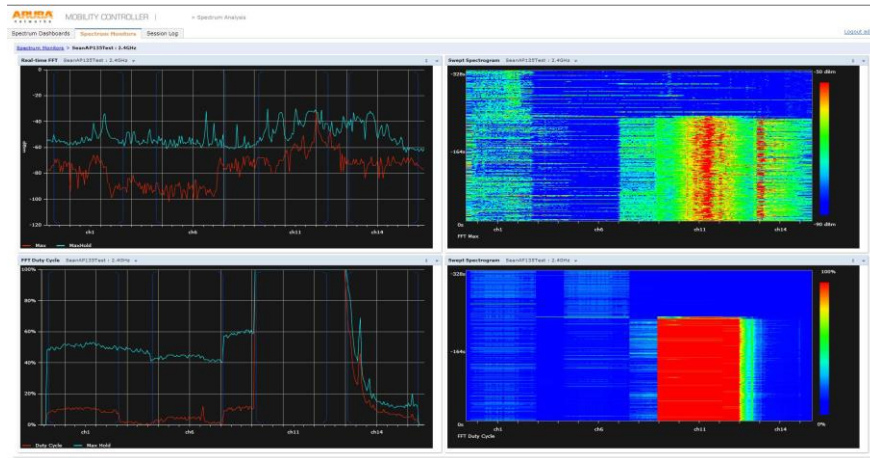
- Remote Spectrum Analysis managed from 1 location



Remote Troubleshooting Kit (RTK). The Sensor AP used for Spectrum Analysis has a Wi-Fi backhaul to the network while roaming (AP is battery powered)



SPECTRUM ANALYZER AP + RADIO/SENSOR



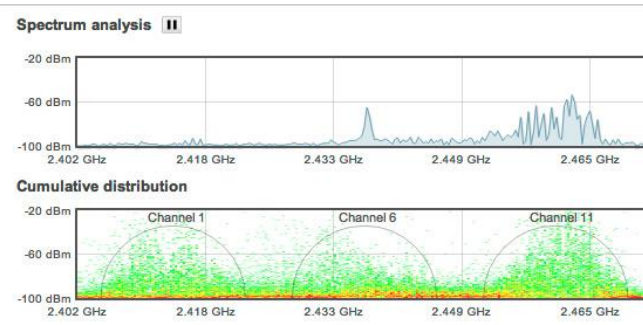
HPE/Aruba Networks – Mobility Controller



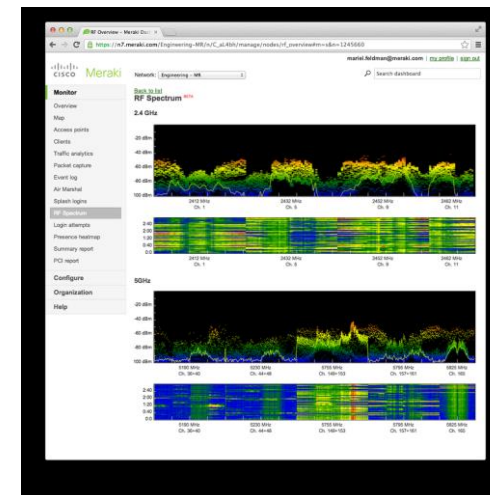
HPE/Aruba Networks – Instant AP

Live tools

- Current clients
- Channel utilization
- Spectrum analysis
- Ping
- Traceroute
- Throughput
- Blink LEDs
- Reboot AP

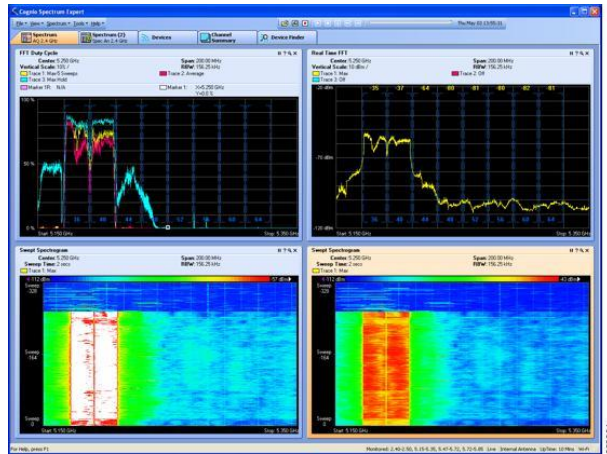


Cisco Meraki – Spectrum Analysis



Cisco Meraki – Spectrum Analysis

SPECTRUM ANALYZER AP + RADIO/SENSOR



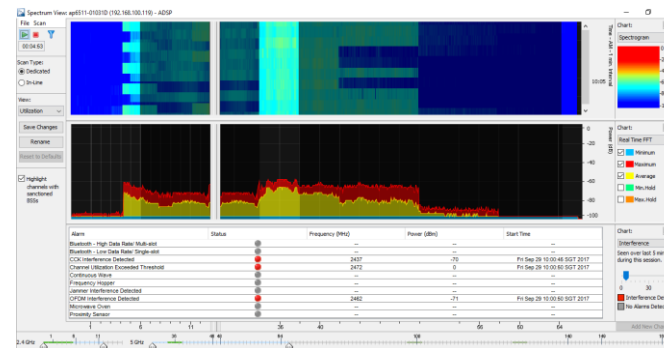
Cisco Spectrum Analysis (“Cognio Chipset”) / Clean Air



Metageek Chanalyzer with Cisco Clean Air

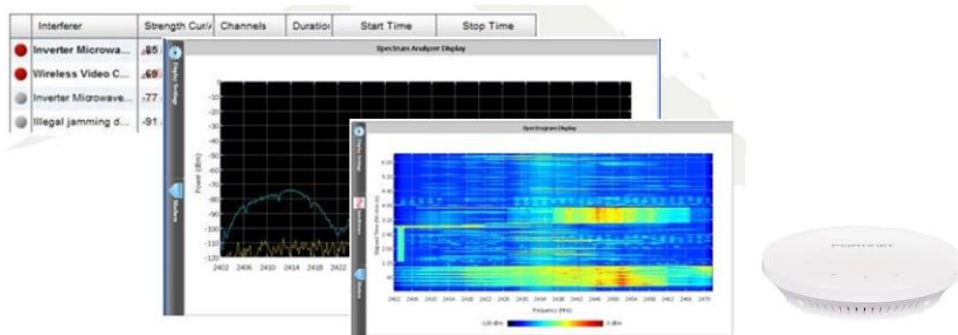


Arris/Brocade Ruckus – Spectrum Analysis in Virtual SmartZone (vSZ)

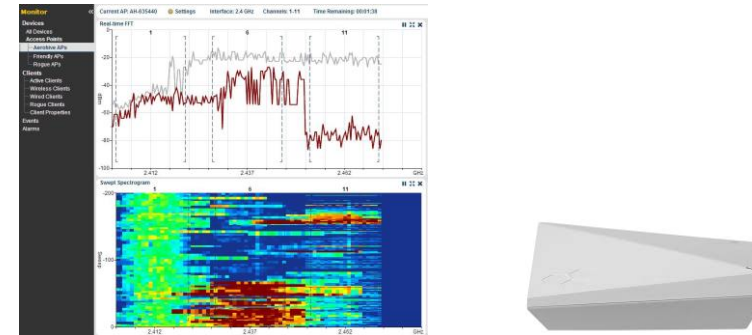


Extreme Networks – AirDefense Services Platform (ADSP)
Note: configurable User Interface

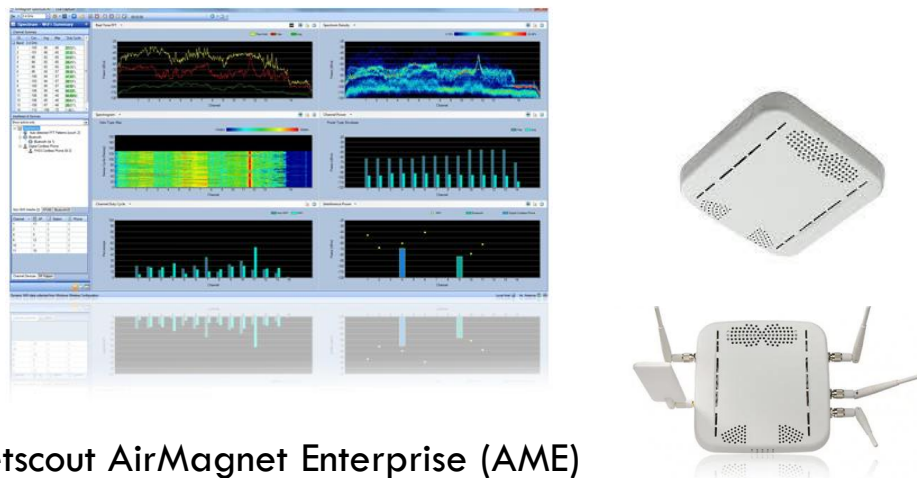
SPECTRUM ANALYZER AP + RADIO/SENSOR



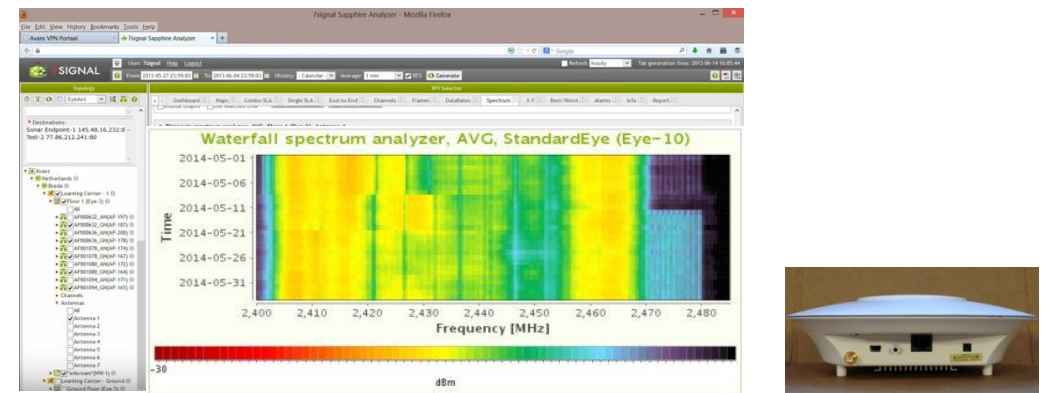
Fortinet (Meru Networks) – Spectrum Analyzer



Aerohive – Spectrum Analyzer



Netscout AirMagnet Enterprise (AME)



7Signal – Sapphire Analyzer
 Wi-Spy/Chanalyzer, Ekahau Site Survey, Cisco CleanAir,
 Oscium Wi-Pry, 7signal Sapphire Eye

OSI LAYER 2 — WI-FI PROTOCOL ANALYSIS

WI-FI DESIGN IMPACTING ROAMING ANALYSIS

- Understand how the Wi-Fi network has been designed
 - Which frequencies (2.4 GHz and/or 5 GHz) are used for the Wi-Fi network?
 - Which channels are used? (are the channels fixed or dynamically controlled?)
 - In 5 GHz think about DFS (Dynamic Frequency Selection) of AP and clients
 - Density of the Access Points (AP)s and if there are “overlapping” channels
 - Impact of Co-Channel Interference (CCI) and Client Induced Interference (CII)
 - Radio Frequency (RF) coverage areas and related signal strengths (higher requirements for Voice)
 - Depending on the roaming solution used and supported by both client and Access Points (AP) also Security has an impact (as security keys sometimes need to be cached)

RESOURCES — IEEE 802.11 TECHNOLOGIES

WI-FI ROAMING

- Wi-Fi Trek 2016 New Orleans, by David Coleman CWNE #4 (Aerohive Networks, USA)

Rome wasn't built in a day...and neither is roaming!

<https://www.cwnp.com/nola-ppt-pdfs/WedPresentations/David%20Coleman%20-%20Roam%20Wasnt%20Built%20in%20a%20Day.pdf>

- Rasika Nayanajith CWNE #153 (La Trobe University, Melbourne, Australia)

Protocol captures (Cisco Controller/AP and Wireshark)

Study material extracts of Sybex CWSP-204/205 material

<https://mrncciew.com/2014/09/13/how-to-study-for-cwsp/>

- See Apple iPhone and different IOS roaming decisions (Ekahau Webinar)

https://www.youtube.com/watch?time_continue=1452&v=PPsanuS-i8A

Jerome Henry CWNE #45

- Ekahau Webinar - Bryan Harkins CWNE #44 - Planning AP placement for roaming and resiliency

<https://www.youtube.com/watch?&v=2iq6s9dIG0>

CH7- 802.11 Fast Secure Roaming
1. CWSP- RSNA
2. CWSP- 802.11 Roaming Basics
3. CWSP- PMK Caching & Preauthentication
4. CWSP- Opportunistic Key Caching (OKC)
5. CWSP- 802.11r Key Hierarchy
6. CWSP- 802.11r FT Association
7. CWSP- 802.11r Over-the-Air Fast BSS Transition
8. CWSP- 802.11r Over-the-DS Fast BSS Transition
9. CWSP- 802.11k AP Assisted Roaming
10. CWSP- Voice Personal & Voice Enterprise

RESOURCES — CLIENT ADAPTERS

WI-FI ROAMING

Roaming Tendency
Roaming Sensitivity (or Policy or Mode or Aggressiveness)
Roaming Decision
Roaming Preference

- Table by Ronald van Kleunen CWNE #108, Globeron
- <https://docs.google.com/spreadsheets/d/1G34wz1RRI6gJ4zBhR6vwwU3aZfVEeKTGfe5Ouhv476s/edit#gid=37929232>
- Windows / Apple / Linux - If supported or if the right driver is used for the Wi-Fi adapter, then Roaming settings can be tuned. e.g. “roaming aggressiveness”. However there is not much information available how the “roaming algorithm or decision works” (usually signal strength RSSI, sometimes bandwidth, data rate, etc. CER, etc.)
- Smartphones / Tablets (Android / IOS)
- Device support for Spectrum / Frequency ranges 2.4 GHz and 5 GHz
(and roaming support between the frequencies if needed)
- Switch / Roaming between Cellular/Mobile (non-Wi-Fi) and Wi-Fi networks

INFO FROM TAMOSOFT - COMMVIEW




- **1. Power consumption.** A single adapter might need up to 450 mA of power. A single USB 2.0 port can provide up to 500 mA. A single USB 3.0 port can provide up to 900 mA. A typical modern laptop has two USB 3.0 ports, so you should either use one adapter per port, or you can use a USB hub, but if you plug in three adapters into a USB 3.0 hub, you will exceed the 900 mA limit, which might cause undesirable effects, e.g. the adapters might stop capturing packets silently.
- **2. Channel switching time.** When CommView for WiFi is working in scanner mode, switching channels takes some time, between 20 and 80 milliseconds per adapter. Consider a scan of 12 channels with the scanner interval of 250 ms per channel and the channel switch time of, say, 60 ms. The total time would be $(250 + 60) * 12 = 3.72$ seconds if you use a single adapter. If you use three adapters, the total time would be $(250 + 60 * 3) * 4 = 1.72$ seconds. That is x2.16 times better, not x3 times better. Thus, adding adapters adds channel switching overhead. If you use 12 adapters, which is possible in theory, it will take $250 + 60 * 12 = 0.97$ seconds to scan 12 channels, so you're not gaining much.

INFO FROM SAVVIUS - OMNIPEEK

WildPackets

USB

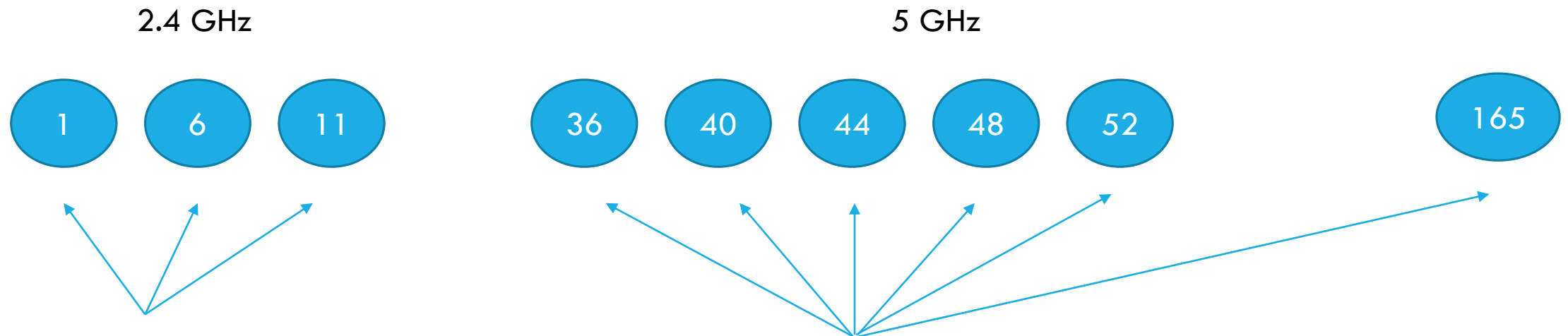
- **USB 1.1 (Full Speed)**
 - September 1998
 - 12 Mbps
 - If you still have equipment with v1.1, get something new!
- **USB 2.0 (High Speed)**
 - April 2000
 - 480 Mbps theoretical; 280 Mbps effective
 - Extremely common for laptops in use
- **USB 3.0 (Super Speed)**
 - November 2008
 - 5 Gbps theoretical; 3.2 Gbps effective

#wp_80211ac

© WildPackets, Inc.

CAPTURE SIMULTANEOUSLY ON ALL CHANNELS



Capture simultaneously
To do roaming analysis
(requires "3" adapters to capture)

Capture simultaneously
To do roaming analysis
(requires 5 adapters .. or more to capture)

HARDWARE + SOFTWARE — OSI LAYER 2

LAPTOP BASED TOOLS

Portable – Protocol Analyzers Supporting 3 or more adapters to capture simultaneously

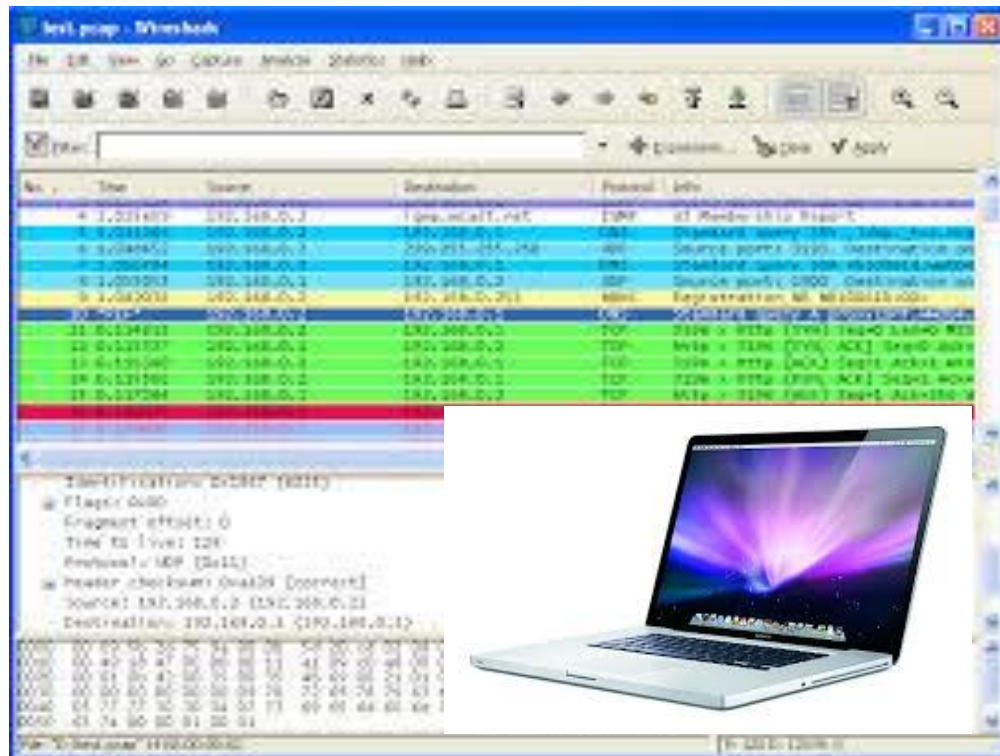
- Savvius Omnipeek + many adapters are supported
- Tamosoft Commview + many adapters are supported (only of the same chipset) + Spectrum analysis (Wi-Spy DBx adapter)
- Netscout Wi-Fi Analyzer + max. 3 adapters (of the same chipset)
- Tshark (command line version of Wireshark), can capture simultaneously by running multiple instances

Portable – Protocol Analyzers Supporting 1 adapter (cannot capture simultaneously)

- Wireshark
 - Apple – integrated adapter (built-in MacBookPro)
 - Windows + AirPCAP or NDIS driver
 - Linux + linux driver to put adapter in monitor mode
- Extreme Networks – AirDefense Mobile + adapter (e.g. Ubiquiti SR71 / Proxim WD8494 / Ekahau-NIC 300)
- Acrylic Wi-Fi Pro + adapter that supports monitor mode (e.g. Proxim WD8494/Ekahau-NIC300/etc) + NDIS capture
- Eye P.A. (Packet Analyzer) + AirPcap adapter

HARDWARE — OSI LAYER 2 — LAPTOP BASED TOOLS

- Protocol Analyzers / Packet Capture tools
- Wireshark on Apple Mac Book Pro



- Protocol Analyzers / Packet Capture tools

- Apple Mac OS X (MacBookPro) has a built-in Broadcom chipset. The OS supports natively packet captures and therefore no external adapters or dongles are required. The chip will be in monitor mode and captures frames on channel only (or multiple channels, but then you are missing frames)

- Capture 802.11ac (and backwards .11n, etc.)
- Capture up to 3x3:3 (80 MHz) = 1300 Mbps
- Use Airtool for easy configuration of Wireshark <https://www.adriangranados.com/apps/airtool>
- Additional Wi-Fi USB adapters can be installed, but not in monitor mode (as drivers cannot be installed).

Note:

To do roaming analysis you want to capture concurrently on multiple channels, but this cannot be done in Wireshark or natively in Mac OS X. Other tools need to be used in a VM-box environment (Linux or Windows).

HARDWARE – OSI LAYER 2 – LAPTOP BASED TOOLS



- Protocol Analyzers / Packet Capture tools
- Wireshark on Windows 10

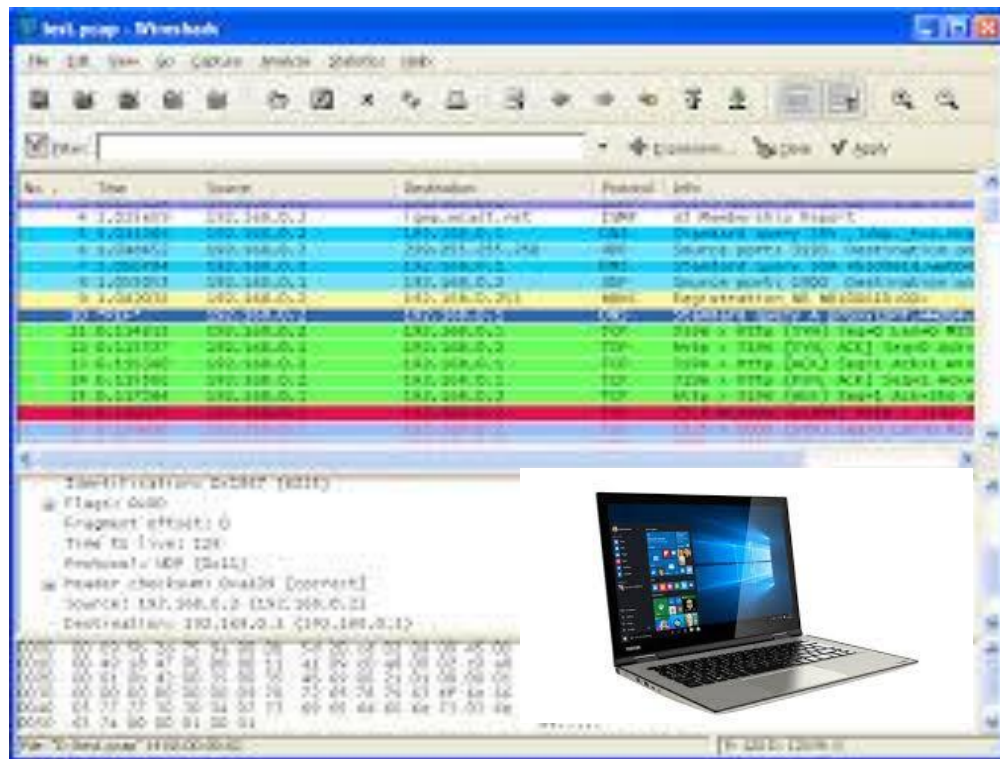
- Protocol Analyzers / Packet Capture tools

- Windows 10 requires an external adapter. Typically the AirPCAP adapter of Riverbed is used, but it only supports IEEE 802.11n (2x2:2) streams only (300 Mbps) and therefore cannot capture 3x3:3 .11n or .11ac type of data frames.

The following solutions also work, but give some frame check sequence errors:

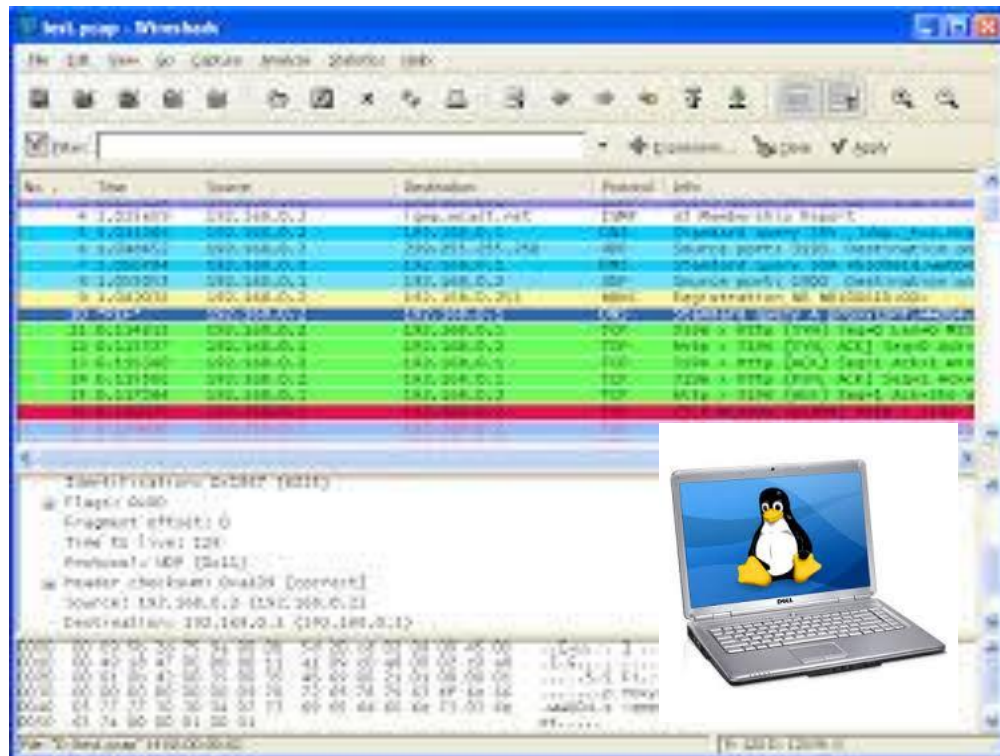
- There are other OEMs of this chipset AR9170/AR9104 (like Proxim WD8494, Ekahau NIC 300, D-Link DWA-160 Ax, Ubiquiti SR-71 USB and more) and with the right driver you can capture frames into Wireshark with the NDIS drivers
- Also with the Asus .11ac 2x2:2 it is possible using the NDIS drivers in Windows
https://wikidevi.com/wiki/ASUS_USB-AC53

Note: To do roaming analysis you want to capture concurrently on multiple channels, but this cannot be done in Wireshark?



HARDWARE — OSI LAYER 2 — LAPTOP BASED TOOLS

- Protocol Analyzers / Packet Capture tools
- Wireshark on Linux



- Protocol Analyzers / Packet Capture tools

- Linux is more flexible and drivers can be installed and adapters can be put into monitor mode if the adapter supports it. (wikidevi has the drivers) and now captures with USB devices supporting 4x4:4 .11 ac can be done (up to 1733 Mbps)

- but you can also use these chipset AR9170/AR9104 (like Proxim WD8494, Ekahau NIC 300, D-Link DWA-160 Ax, Ubiquiti SR-71 USB and more) but limited to 802.11n 2x2:2 (300 Mbps)

- You can run Linux in a VM (e.g. on Windows or Apple MAC OS X platforms) and connect the adapter to the VM to use the adapter in monitor mode

- As platform you can also use a Raspberry PI or Odroid device, which can run Linux natively



HARDWARE — OSI LAYER 2 — LAPTOP BASED TOOLS

- **Protocol Analyzers / Packet Capture tools**
- Wireshark - utilizing an external AP to capture

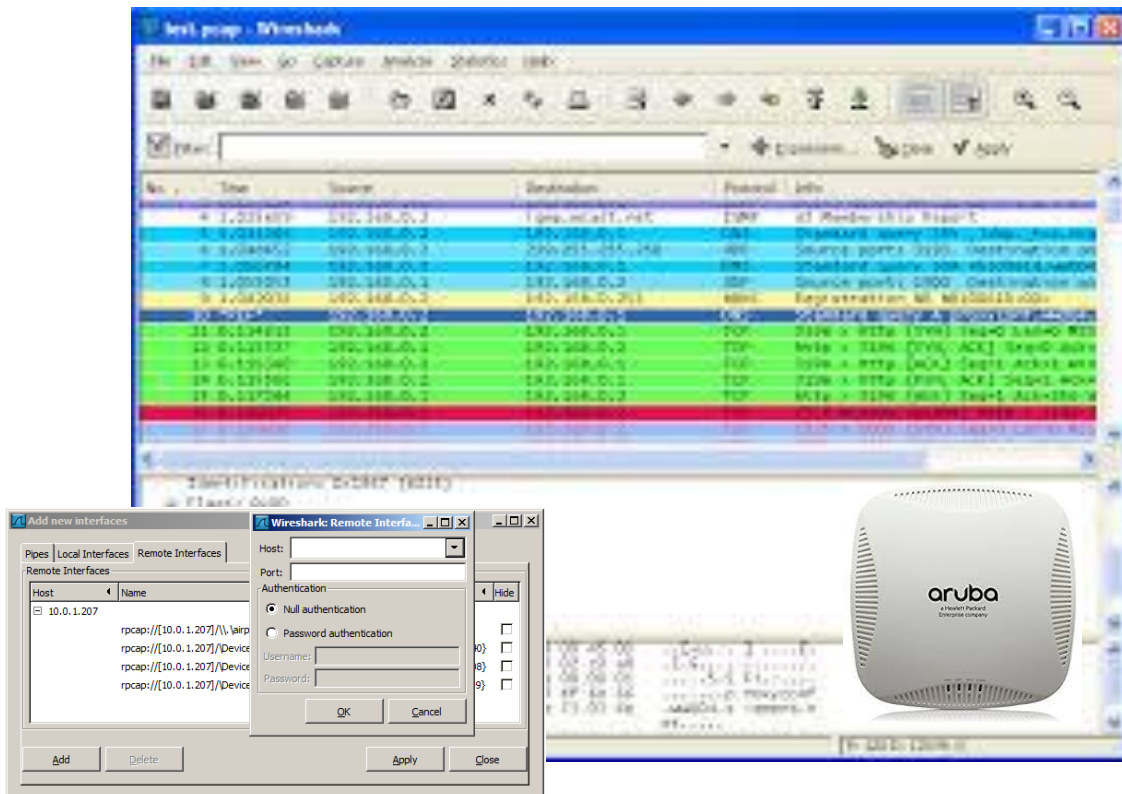
- **Protocol Analyzers / Packet Capture tools**

- If the Access Point (AP) supports monitor mode on the Radio AP chipset and Remote Protocol Analysis (RPCAP) then you can forward the Wi-Fi frames to Wireshark

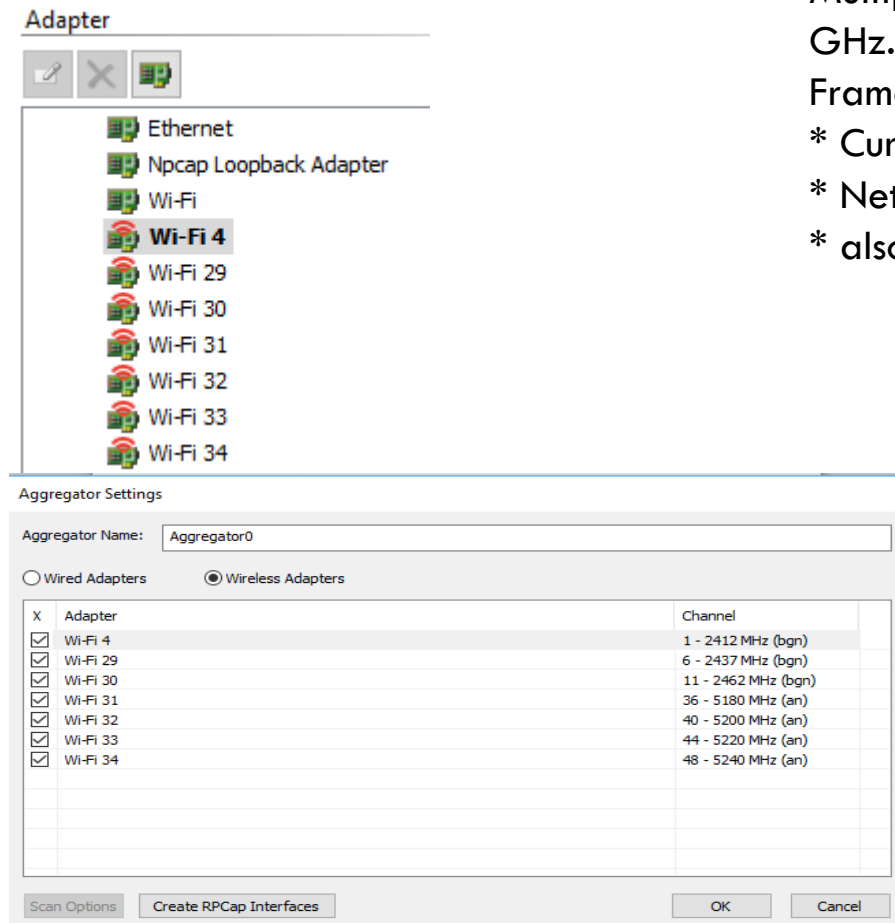
- Here is an example how to do an .11ac 3x3:3 capture by Peter MacKenzie CWNE #33
<https://pnmackenzie.tumblr.com/post/76777894866/3-stream-80211ac-packet-capture-with-the-aruba>

- As it becomes more difficult to capture with USB adapters the upcoming technologies (like 4x4:4 and .11ax upstream/downstream). With the AP option 4x4:4 (or MU-MIMO) and upcoming .11ax if the chipset can be put into monitoring mode.

Note: Wireshark cannot capture multiple sessions (e.g. 2x APs forwarding data to Wireshark to do roaming analysis).



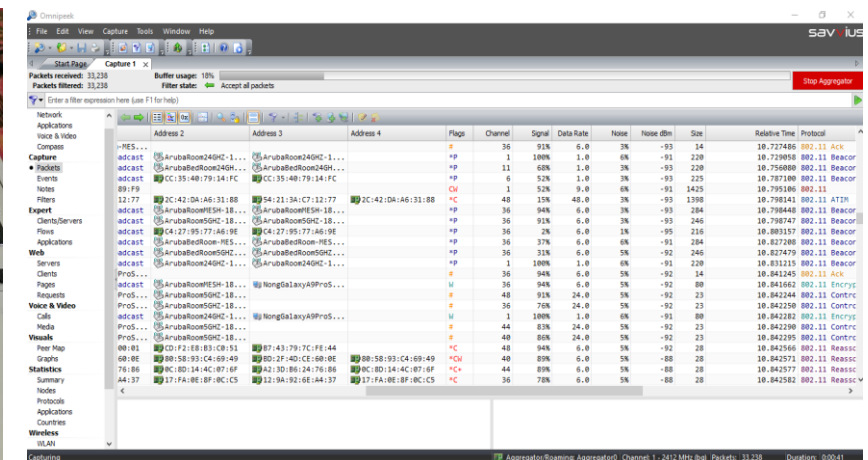
SAVVIUS OMNIPEEK – SUPPORTS AGGREGATOR MODE (SUPPORTS MANY ADAPTERS)



Multiple adapters are supported to do simultaneously packet captures in 2.4 GHz and 5 GHz.

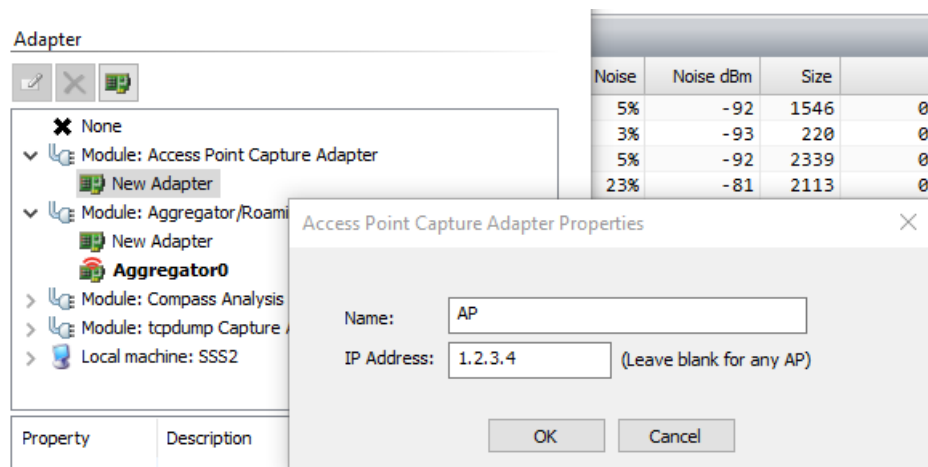
Frame Aggregation (in this case utilizing 7 adapters, but more are possible)

- * Current dongles supported RealTek RT2870/OmniWiFi .11n 3x3:3 (450 Mbps)
- * Netgear 6210 .11ac 2x2:2 (867 Mbps)
- * also think about the USB 3 hub capacity/connection for throughput and power!



SAVVIUS OMNIPEEK – SUPPORTS AP CAPTURE (RPCAP)

- Protocol Analyzers / Packet Capture tools
- Omnipeek - utilizing an external AP to capture

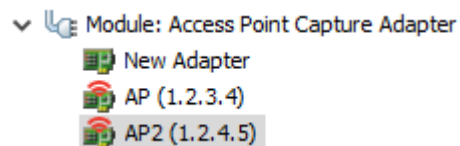


- Protocol Analyzers / Packet Capture tools

- If the Access Point (AP) supports monitor mode on the Radio AP chipset and Remote Protocol Analysis (RPCAP) then you can forward the Wi-Fi frames to Omnipeek

- Here is an example how to do an 802.11ac 3x3:3 capture by Peter MacKenzie CWNE #33
<https://pnmackenzie.tumblr.com/post/76777894866/3-stream-80211ac-packet-capture-with-the-aruba>

- As it becomes more difficult to capture with USB adapters the upcoming technologies (like 4x4:4 and 802.11ax upstream/downstream). With the AP option 4x4:4 (or MU-MIMO) and upcoming 802.11ax if the chipset can be put into monitoring mode.



Omnipeek can capture multiple sessions (e.g. 2x APs forwarding data to Omnipeek to do roaming analysis).

NETSCOUT — AIRMAGNET WI-FI ANALYZER

ROAMING ANALYSIS

Roaming Analysis

All Roaming Events

Roaming Start Time	Roaming End Time	Delay(ms)	Delay Rating	Device Name	AP Name (From)	CH (From)	AP Name (To)	CH (To)	Signal d...	Signal d...	MOS (...)	MOS (...)
Data Roaming Events												
09/29 12:47:23.980	09/29 12:47:28.717	4736	N/A	Hon Hai Precisio:21:CB...	Aruba Networks:D3:D...	36	Aruba Networks:FF:EE...	36	-36	-65	N/A	N/A
09/29 12:48:43.372	09/29 12:48:47.436	4063	N/A	Hon Hai Precisio:21:CB...	Aruba Networks:FF:EE...	36	Aruba Networks:D3:D...	36	-66	-36	N/A	N/A
09/29 12:49:57.276	09/29 12:50:01.764	4488	N/A	Hon Hai Precisio:21:CB...	Aruba Networks:D3:D...	36	Aruba Networks:FF:EE...	36	-35	-66	N/A	N/A
09/29 12:51:14.506	09/29 12:51:18.350	3844	N/A	Hon Hai Precisio:21:CB...	Aruba Networks:FF:EE...	36	Aruba Networks:D3:D...	36	-63	-34	N/A	N/A

Roaming Reason

Active APs

Hon Hai Precisio:21:CB:77

AirWISE Roaming Reasons

The STA may have initiated roaming for one of the following reasons:

- AP Associated Clients

Station Parameters(Performance)

Name	Before Roaming	After Roaming	Rating
Signal Strength(dBm)	-100 (No Trans...	-23	👍

AP Parameters(Reason)

Name	From AP Aruba...	To AP Aruba...	Rating
Associated Clients	3	1	👍
Retry Rate(%)	0	0	👍
Signal Strength(dBm)	-36	-65	👍

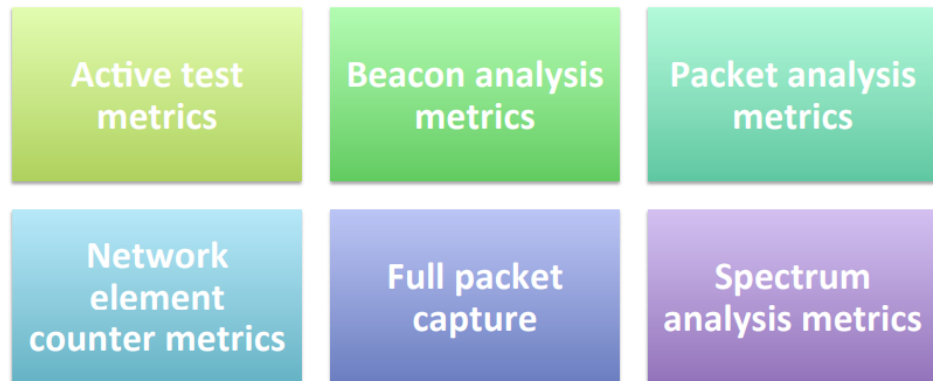
Channel Parameters(Reason)

Name	From CH 36	To CH 36	Rating
Active APs	5	5	👍
Active Clients	4	4	👍
Interference	0	0	👍

6 | 1 | 36 | 1.4% [7/512 MB]

7SIGNAL – SENSORS (“EYE”) SUPPORT PACKET CAPTURE USED FOR ANALYSIS AND ALSO CAN BE IMPORTED IN TOOLS THAT SUPPORT PCAP FORMAT

Data collection methods



Data collection tools



Type of metric	Examples
Active test	iPerf, IxChariot, Ekahau Site Survey, AirMagnet Survey, Speedtest app, nPerf app, 7signal Sapphire, 7signal Mobile Eye app
Beacon analysis/ "Wi-Fi scanners"	Ekahau Site Survey, AirMagnet Survey, Fluke Aircheck, Metageek InSSIDer, Wi-Fi Explorer, Wi-Fi Signal, Acrylic Wi-Fi, CommView, 7signal Sapphire
Packet analysis	Omnipeek, Metageek Eye P.A., 7signal Sapphire
Network element counter	Cisco Prime, Aruba Airwave, Netscout (Netflow, SNMP)
Full packet capture	AP in capture mode, Mac, Wireshark, Omnipeek, 7signal Sapphire
Spectrum analysis	Wi-Spy/Chanalyzer, Ekahau Site Survey, Cisco CleanAir, Oscium Wi-Pry, 7signal Sapphire

Detailed statistics

Ref: <https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/VPKetonenPhoenixWi-Fiperformancev10-1.pdf>

TAMOSOFT COMMVIEW



Spectrum analysis with Wi-Spy DBx



CommView for WiFi - Evaluation Version - Atheros 802.11n Wireless Network Adapter (6)

File Search View Tools Settings Rules Help

Nodes Channels Latest IP Connections Packets VoIP Logging Rules Alarms

Utilization, 2.4 GHz, Mbytes/sec

Utilization, 5.0 GHz, Mbytes/sec

Signal Level, 2.4 GHz, dBm

Signal Level, 5.0 GHz, dBm

Standard / MAC Address	Channel	Type	SSID	Standard	Encryption	Signal
802.11g						
SenaInt:6A:7C:7B	6	AP	LeeHouseWiFi2	802.11g		-85/-83/-80
802.11n						
Technico:79:14:FC	6	AP	110/150	802.11n	WPA-CCMP,W...	-74/-68/-64
E4:8D:8C:16:5B:88	11 (7-11@40)	AP	Hcondo_Swimming	802.11n	WPA-CCMP	-86/-85/-84
D4:7B:B0:B8:D4:F8	11	AP	Gonzales Home Wifi	802.11n	WPA-CCMP,W...	-88/-86/-85
D4:7B:B0:B8:D4:92	11	AP	true_home2G_ACG	802.11n	WPA-CCMP,W...	-90/-84/-78
AskeyCom:3E:88:A3		STA				-87/-79/-76
D-LinkIn:AD:11:45	6	AP	704	802.11n	WPA-CCMP,W...	-85/-84/-84
C0:25:E9:34:DA:B0	11	AP	Alan Extreme_EXT	802.11n	WPA-CCMP,W...	-88/-86/-85
70:5A:9E:D2:18:C5	11	AP	true_home2G_173	802.11n	WPA-CCMP,W...	-85/-73/-67
40:E3:D6:FF:EE:A2	11	AP	www24GHZ	802.11n	WPA-CCMP	-89/-57/-55
24:A2:E1:EA:EB:DE	1	AP	BERLIN_BKK	802.11n	WPA-CCMP	-82/-77/-74
18:64:72:D3:D9:62	1	AP	www24GHZ	802.11n	WPA-CCMP	-38/-35/-31
10:62:EB:90:C1:7C	1	AP	201	802.11n	WPA-CCMP	-87/-84/-83
10:62:EB:90:C0:74	1	AP	CC283	802.11n	WPA-CCMP,W...	-85/-85/-85
0C:D6:BD:35:58:3A	1	AP	ROOM 702	802.11n	WPA-CCMP	-86/-85/-83
0C:D6:BD:35:58:13	1	AP	ROOM 603	802.11n	WPA-CCMP	-84/-82/-81

Channels and Spectrum

Capture: On | Packets: 8,748 | Keys: None | Auto-saving: Off | Rules: Off | Alarms: Off

37% CPU Usage | PR.REQ

Single channel mode

5 GHz - 12
5 GHz - 16
5 GHz - 36
5 GHz - 40
5 GHz - 44

Seconds per channel: 1

Sec. channel below in 40 MHz mode
Active node discovery

Channel Indicator

FREQ 2,412 CH.I

FREQ 2,437 CH.6

FREQ 2,462 CH.II

FREQ 5,180 CH.36

FREQ 5,200 CH.40

FREQ 5,220 CH.44

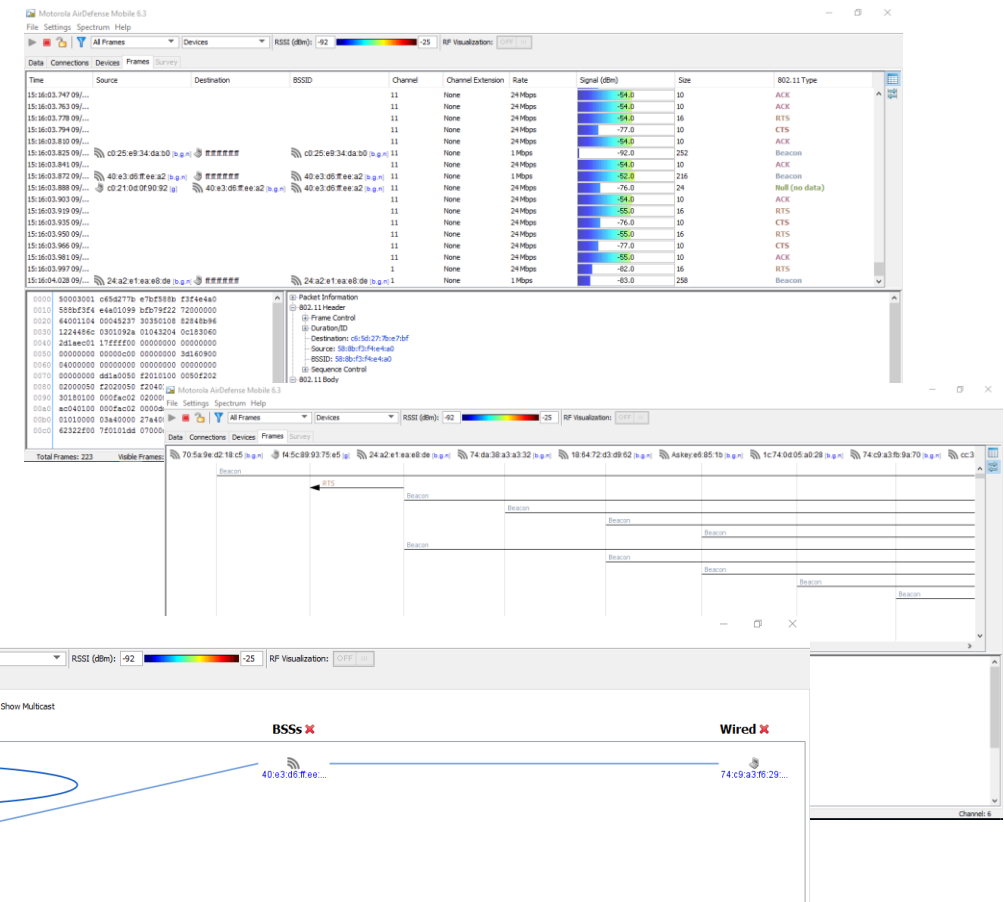
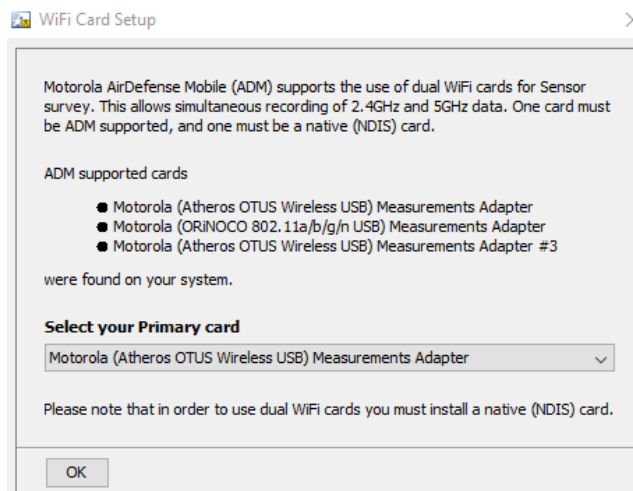
These chipset AR9170/AR9104 (like Proxim WD8494, Ekahau NIC 300, D-Link DWA-160 Ax, Ubiquiti SR-71 USB and more) but limited to 802.11n 2x2:2 (300 Mbps) can be used simultaneously with the right drivers installed. You can do multiple channel captures

EXTREME NETWORKS – AIRDEFENSE MOBILE (SUPPORTS ONLY 1X ADAPTER FOR PROTOCOL ANALYSIS, BUT MULTIPLE FOR SITE SURVEY, INCLUDING NDIS – SEE NEXT SLIDE)

- Only 802.11n 2x2:2 (300 Mbps) adapter

Chipset AR9170/9104

There are other OEMs of this chipset AR9170/AR9104 (like Proxim WD8494, Ekahau NIC 300, D-Link DWA-160 Ax, Ubiquiti SR-71 USB and more) and with the right driver you can capture frames into AirDefense Mobile

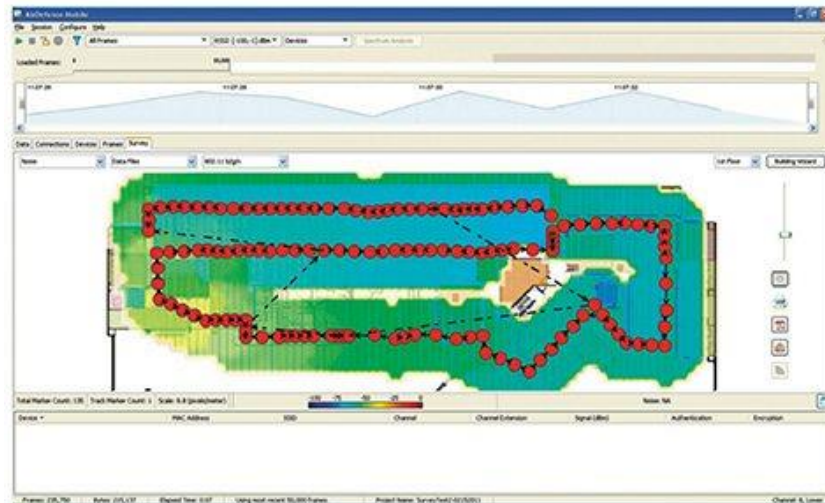
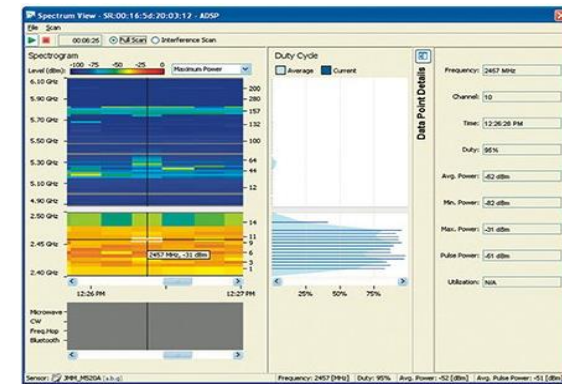


EXTREME NETWORKS – AIRDEFENSE MOBILE

INTEGRATES IN 1 TOOL: PROTOCOL ANALYSIS + SPECTRUM ANALYSIS + SITE SURVEY

- Spectrum Analysis is only supported by a **PCMCIA Cardbus** adapter (requires a laptop with a PCMCIA slot)

Site Survey is supported using multiple dongles NDIS drivers:



ACRYLIC WI-FI PRO

(SUPPORTS 1X ADAPTER IN MONITOR MODE USING NDIS DRIVER)

- Use a driver that works with Acrylic Wi-Fi
 - e.g. an Ekahau-NIC 300 adapter with Ekahau driver then enable in Acrylic Wi-Fi Monitor mode

Then on the top select the 3rd icon (to get the “packet capture view”) and at the right slider “View packets” on

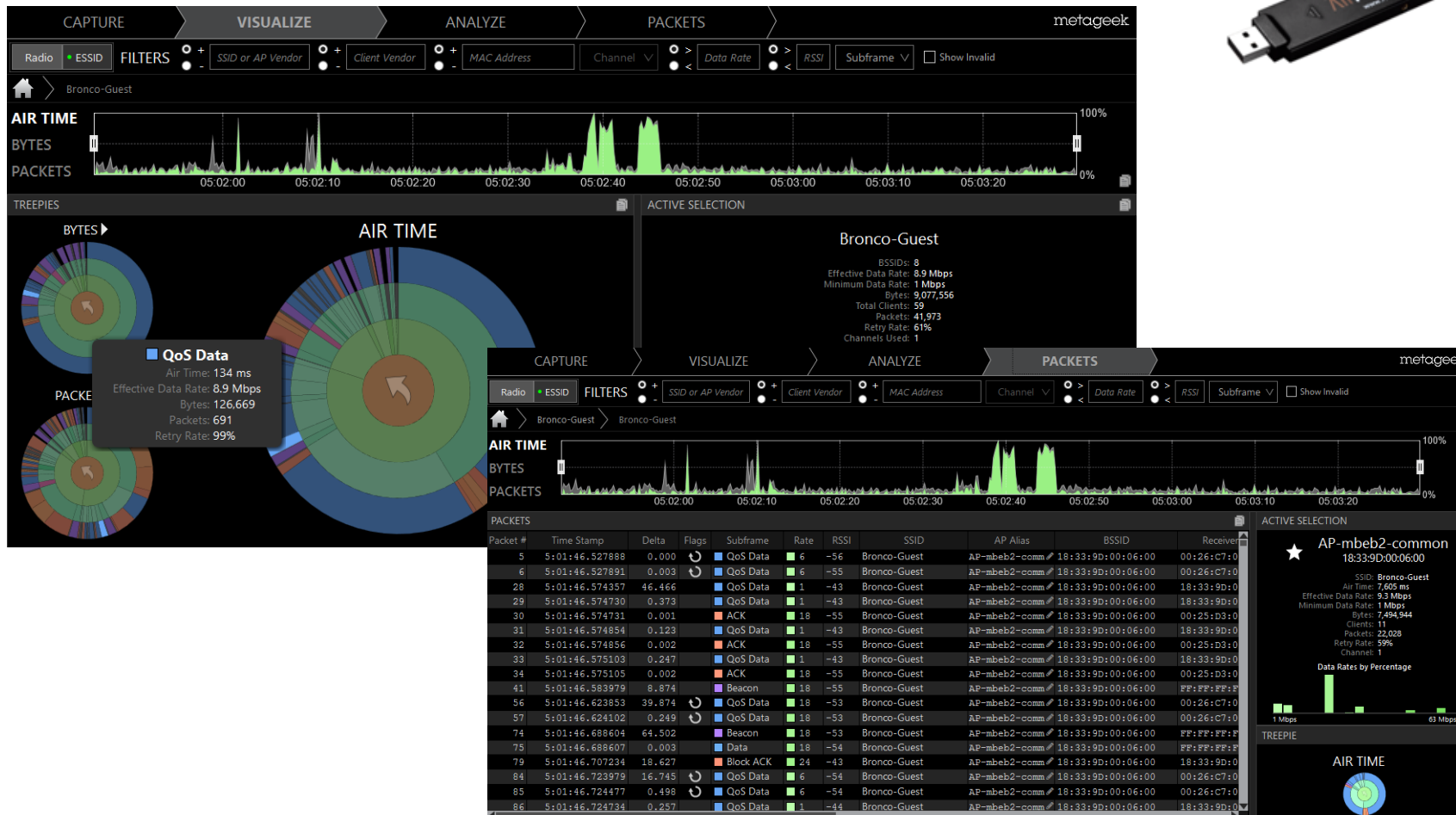
The screenshot shows the Acrylic Wi-Fi Professional interface. At the top, there are icons for Wi-Fi, a mobile phone, a folder (highlighted with a red box), a document, and a globe. Below the icons, the software title 'Acrylic Wi-Fi Professional' is visible. On the right side, there are settings for the NDIS interface, with 'Mode: Monitor' (highlighted with a red box) and a 'Change' button. Below these settings are various options like Channel Hopping, GPS, Packet Viewer (set to On), and Pcap. A 'Windows' menu is open, showing 'Packet Viewer' (highlighted with a red box) and other options like Access Points, Stations, Scripting, News, OWISAM, and Inventory. The main area displays a table of captured packets with columns for Number, Time, RSSI, Chan, Type, SubType, Source Address, BSSID, Destination Address, and Size. The table contains several rows of data, with the 20th row highlighted in yellow.

Number	Time	RSSI	Chan	Type	SubType	Source Address	BSSID	Destination Address	Size
7	25.6383	-73	6	Manaqemen Beacon	Cisco!	Cisco	Cisco	[Broadcast]	225 SS
8	25.6393	-86	6	Manaqemen ProbeRequest	IntelC	[Broa	[Broa	[Broadcast]	97 SS
9	25.6401	-86	6	Manaqemen ProbeRequest	IntelC	[Broa	[Broa	[Broadcast]	97 SS
10	26.3417	-87	10	Manaqemen Beacon	CE:D7	CE:D7	CE:D7	[Broadcast]	33 SS
11	26.3884	-87	10	Manaqemen Beacon	Cisco-	Cisco-	Cisco-	[Broadcast]	104 SS
12	26.4355	-84	10	Manaqemen Beacon	Cradle	Cradle	Cradle	[Broadcast]	24 SS
13	26.5294	-83	11	Manaqemen ProbeRespon	Cradle	Cradle	IntelCor_8	[Broadcast]	115 SS
14	26.5307	-81	11	Manaqemen ProbeRespon	Cradle	Cradle	IntelCor_8	[Broadcast]	115 SS
15	26.5315	-68	11	Manaqemen Beacon	Cisco!	Cisco	Cisco	[Broadcast]	115 SS
16	26.5446	-82	11	Manaqemen ProbeRespon	Cradle	Cradle	IntelCor_8F	[Broadcast]	115 SS
17	26.5460	-68	11	Data	QoSData	Fortin	Cisco	[Broadcast]	115 SS
18	26.5478	-68	11	Data	QoSData	Fortin	Cisco	[Broadcast]	115 SS
19	26.5485	-68	11	Control	Acknowledge				
20	26.5504	-69	11	Control	Acknowledge				
21	26.5511	-69	11	Control	Acknowledge				

METAGEEK EYE P.A.

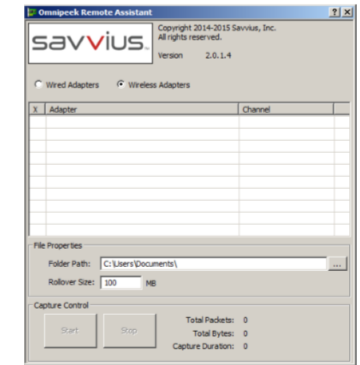
Requires AirPCAP devices

(similar other OEMs with 9170/9104 chipset do not work)



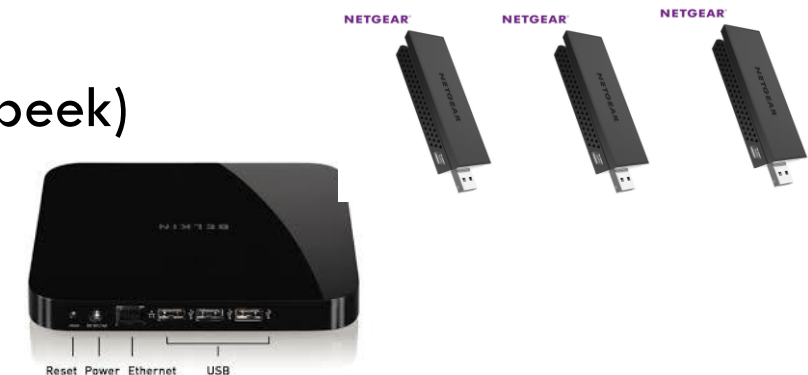
After the capture Eye P.A. can also sent the packets directly to Wireshark (without saving first the pcap file)

HARDWARE + SOFTWARE – OSI LAYER 2 LAPTOP BASED TOOLS



Remote Protocol Analysis / Packet Capture

- Savvius Omnipcap + O.R.A. (built-in software in OmniPeek) – OmniPeek Remote Analysis
- Netscout AirMagnet Wi-Fi Analyzer connecting to a remote AirMagnet Wi-Fi Analyzer installed on a laptop
- Remote – Ethernet connection and remotely connect to USB adapters
requires software on the laptop (Windows and MacOS X)
e.g. Belkin Network USB Hub, F5L009 v1 (works with Omnipcap)



HARDWARE + SOFTWARE – OSI LAYER 2 EMBEDDED BASED TOOLS OPENWRT AND CLOUDSHARK

- <https://wiki.openwrt.org/toh/start>

(Raspberry Pi, Linksys WRT54GL, Wireless home gateways/routers, etc.)

- <https://openwrt.org/>

- <https://support.cloudshark.org/openwrt/openwrt-cloudshark.html>



Raspberry Pi

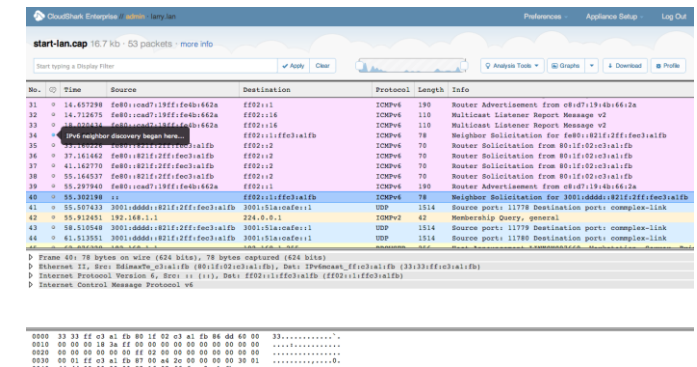


Cisco Linksys WRT54GL



Ubiquiti Edge Router Lite

and many more....



RASPBERRY PI OR ODROID C2 AND USB-ADAPTER SUPPORTING MONITOR MODE

- <http://www.globeron.com/freedownload/services/Globeron-1-2-3-Adapters-Atheros9170AR9104.pdf>

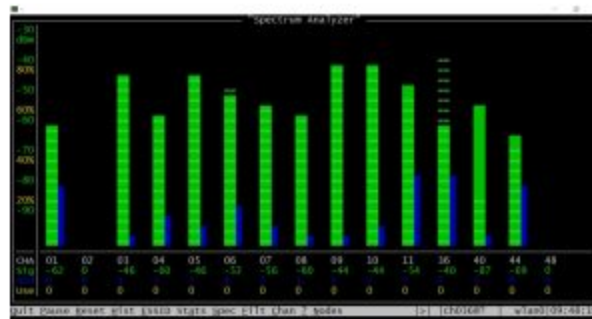


ODROID-C2



NETBEEZ WITH HORST

- <https://netbeez.net/blog/remote-wifi-packet-capturing-with-horst-on-raspberry-pi-and-odroid/>



The **Highly Optimized Radio Scanning Tool (HORST)** is a lightweight IEEE802.11 WLAN analyzer. It was built for **troubleshooting WLAN networks**, and although it's not as advanced as other tools (Kismet, Wireshark, tcpdump) it's very easy to use, free, and can run very efficiently even on a Raspberry Pi.

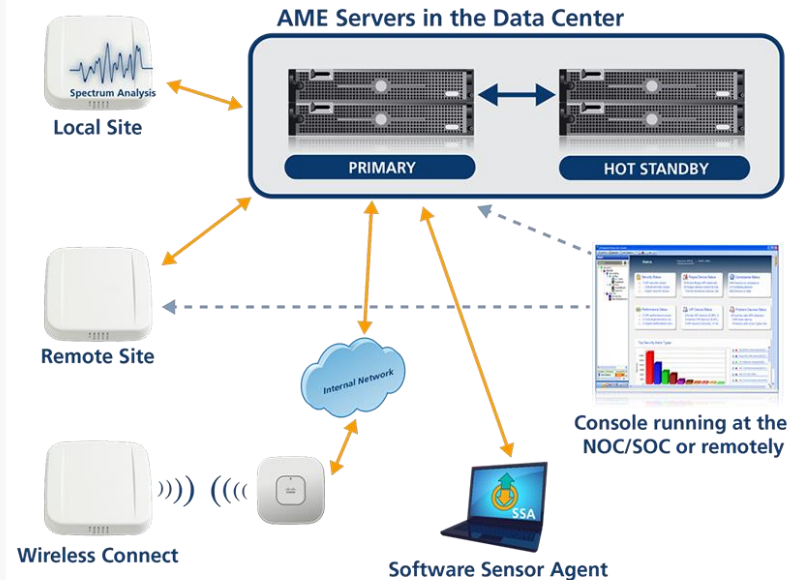
For the installation and usage details, please see HORST on [GitHub](#).

REMOTE PROTOCOL USING AN AP/RADIO SENSOR

- Fixed setup – Remote Protocol Analysis using APs in fixed locations in the office or global locations



- Remote Protocol Analysis managed from 1 location



Remote Troubleshooting Kit (RTK). The Sensor AP used for Protocol Analysis has a Wi-Fi backhaul to the network while roaming (AP is battery powered)



EXTREME NETWORKS — AIRDEFENSE PLATFORM AND MULTIPLE REMOTE AP (“LIVE VIEW”) TO DO REMOTE PROTOCOL ANALYSIS (ALL GUI INTEGRATED)

Live View-ADSP

File Session Scope: ap6511-0303D [a,b,g,n]

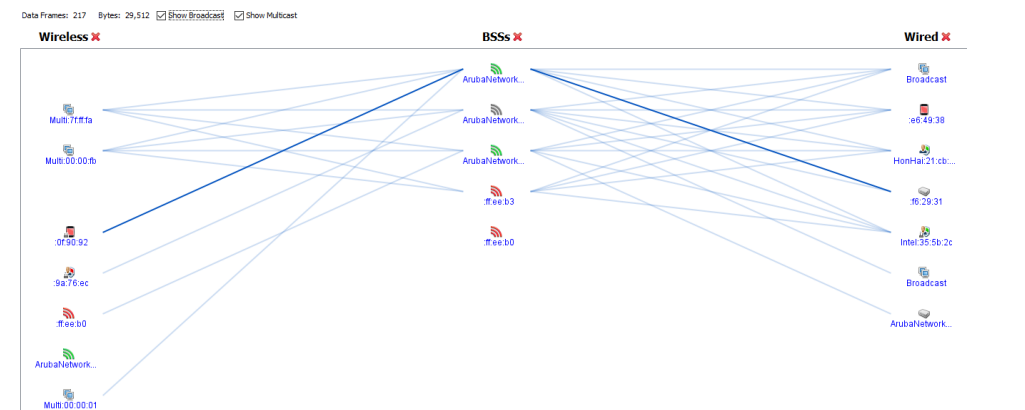
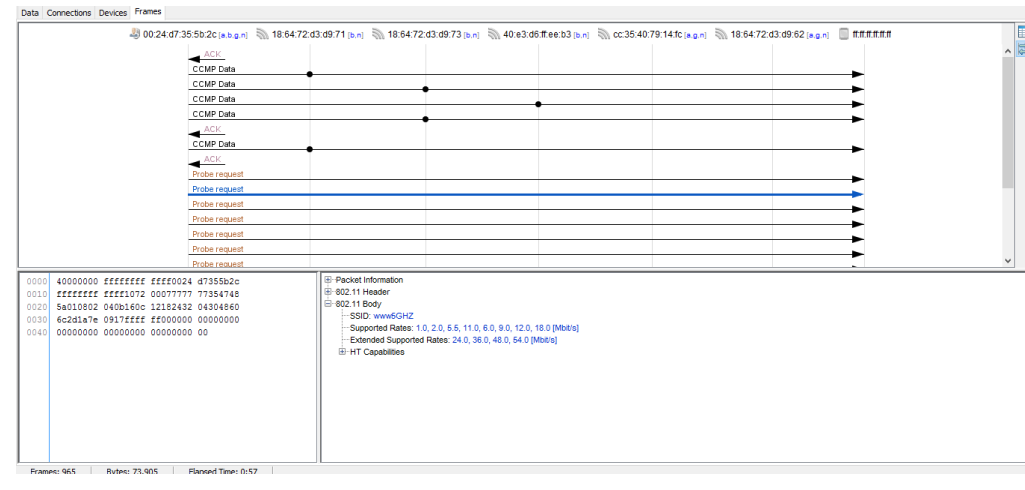
Data Connections Devices Frames

Time	Source	Destination	BSSID	Observed Chan...	Channel Extens...	Rate	Signal (dBm)	Size	802.11 Type	SSID
12:01:21.219 09...	192.168.100.114	Broadcast	192.168.100.114	136	None	6 Mbps	-45	223	Beacon	g80z
12:01:21.229 09...	192.168.100.118	Broadcast	192.168.100.118	136	None	6 Mbps	-45	223	Beacon	g806
12:01:21.239 09...	192.168.100.117	Broadcast	192.168.100.117	136	None	6 Mbps	-50	223	Beacon	g800
12:01:21.329 09...	192.168.100.114	Broadcast	192.168.100.114	136	None	6 Mbps	-52	223	Beacon	g802
12:01:21.329 09...	192.168.100.118	Broadcast	192.168.100.118	136	None	6 Mbps	-45	223	Beacon	g806
12:01:21.429 09...	192.168.100.117	Broadcast	192.168.100.117	136	None	6 Mbps	-52	223	Beacon	g802
12:01:21.439 09...	192.168.100.118	Broadcast	192.168.100.118	136	None	6 Mbps	-45	223	Beacon	g806
12:01:21.529 09...	192.168.100.117	Broadcast	192.168.100.117	136	None	6 Mbps	-50	223	Beacon	g805
12:01:21.529 09...	192.168.100.114	Broadcast	192.168.100.114	136	None	6 Mbps	-51	223	Beacon	g802
12:01:21.539 09...	192.168.100.118	Broadcast	192.168.100.118	136	None	6 Mbps	-45	223	Beacon	g806
12:01:27.699 09...	80.1f02:bc:93:38	Broadcast	80.1f02:bc:93:38	48	None	6 Mbps	-56	64	Probe request	
12:01:27.699 09...	80.1f02:bc:93:38	Broadcast	80.1f02:bc:93:38	48	None	6 Mbps	-56	64	Probe request	
12:01:27.619 09...	80.1f02:bc:93:38	Broadcast	80.1f02:bc:93:38	48	None	6 Mbps	-55	64	Probe request	
12:01:28.969 09...	TechnicolorUsa.79.1.._e	Broadcast	TechnicolorUsa.79.1.._e	None	1 Mbps	-52	-21	221	Beacon	110180
12:01:28.969 09...	TechnicolorUsa.79.1.._e	Broadcast	TechnicolorUsa.79.1.._e	None	1 Mbps	-54	-21	221	Beacon	110180
12:01:29.179 09...	TechnicolorUsa.79.1.._e	Broadcast	TechnicolorUsa.79.1.._e	None	1 Mbps	-52	-21	221	Beacon	110180

0000 40000000 ffffffff ffff50e b8eacde0
 0011 50e8bec ede002b 3ba07729 00000000
 0021 6400181 0005676c 62303501 089c1298
 0031 24004860 60505401 02000007 12474249
 0041 24041734 04176460 1e79031e 84031e20
 0051 01000b05 00000112 7a2d1a0c 0017ffff
 0061 00000000 00000000 00000000 00000000
 0071 00000000 003a1e88 08400000 00000000
 0081 00000000 00000000 00000000 004a0e14
 0091 000a00b4 00140014 0002000a 00720601
 00a1 00000000 00a82000 40f80000 03001300
 00b1 00002551 ca59a807 00020202 00010a8d
 00c1 1e00a0f8 03000100 00000000 00000000
 00d1 00000000 0050e8b0 e6c8ba00 001488

802.11 Body
 -Timestamp: 69705669
 -Beacon Interval: 100
 -Capability Information
 -SSID: g805
 -Supported Rates: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 64.0 [Mbps]
 -Traffic Indication Map
 -Country
 -Power Constraint
 -BSS Load
 -HT Capabilities
 -HT Information
 -Unknown Element: id = 74
 -Unknown Element: id = 173
 -Vendor Specific Information: 4 bytes (CUI: 0x000000)

Frames: 727 Bytes: 32,755 Elapsed Time: 0:21



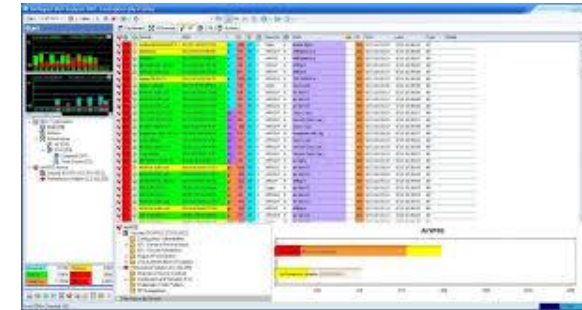
AP + RADIO/SENSOR IN MONITOR / PROTOCOL CAPTURE MODE



- Set a radio on the FortiAP to monitor mode.

```
iwconfig wlan0
Result:
wlan0 IEEE 802.11na ESSID:""
Mode:Monitor Frequency:5.18 GHz Access Point: Not-Associated
```

- The capture file is stored under the temp directory as w1_sniff.pcap /tmp/w1_sniff.pcap
 - Remember that the capture file is only stored temporarily. If you want to save it, upload it to a TFTP server before rebooting or changing the radio settings.
 - The command `cp w1_sniff.pcap newname.pcap` allows you to rename the file.
 - Rather than TFTP the file, you can also log in to the AP and retrieve the file via the web interface. Move the file using the command: `mv name /usr/www` You can verify the file was moved using the command `cd /usr/www` and then browsing to: `<fortiAP_IP>/filename`



Fortinet (Meru Networks) Monitor mode on FortiAP and TFTP and Wireshark

Netscout AirMagnet Enterprise (AME) and dual band sensors

<http://wlanimp.blogspot.com/2014/04/capturing-80211-frames-with-ruckus.html>



Arris/Brocade Ruckus – Protocol Streaming to Wireshark

WING 5 now gives a network administrator fully distributed packet capture capabilities to perform troubleshooting at a very granular level. The following diagram represents points at which packet capture can be executed as related to an access point running WING 5; every logical and physical boundary can facilitate captures in both inbound and outbound directions:

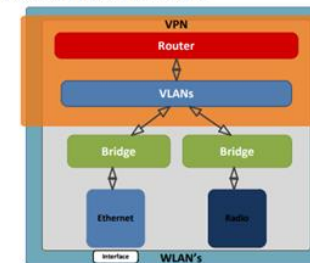


Figure 1: Points of Capture Logical Diagram



Extreme Networks – WING 5 pktcap to pcap file and capture to remote destinations (tftp, ftp or a Tazman Sniffer Protocol (tzsp) host via the remote-debug command)

SESSION - PROTOCOL CAPTURES ON 2.4 GHZ AND 5 GHZ (CAPTURE IS BASED ON VIEW)

- Capture everything (changing Wi-Fi Channels), or only per Channel, AP, Client, etc.
- Sessions are saved on the AirCheck G2 and can be exported to USB in pcap format
- These can be imported into tools that support PCAP format, like Wireshark, Omnipcap, etc.





1

2

3

WI-FI ROAMING ANALYSIS TOOLS HARDWARE / SOFTWARE REQUIREMENTS

1-2-3 with Globeron

