Instant AP Packet Capture.

You will need:

- An instant IAP
- Access to the GUI of the Instant AP
- Access to the commandline of the Instant AP
- A separate management station, capable of installing and running Wireshark. The management station should have the firewall disabled or be able to receive traffic from UDP 5555

Get into the IAP GUI Navigate to the AP > edit > Radio tab > Mode. Change to Monitor and click OK.

Reboot the AP for the change to take effect

🔊 1 Access Po	bint	+ 📕 5 Clients Associat
Name 🗸	Clients	Name - II
00:24:6c:cb:30:cd	5 <u>edi</u>	
	Edit Access Point 00:24:6	c:cb:30:cd Help
	General Radio Uplink	
	Mode: Access Access 2.4 GH Monitor Spectrum Monitor	assigned
	Administrator assigned	
	Channel: 1	
	Transmit power: d	dBm
	5 GHz band	
	Adaptive radio management a	assigned
	Administrator assigned	
	Channel: 36 👻	
	Transmit power:	dBm
ghboring APs		OK Cancel

*You need to reboot for the radio change to take effect. So reboot the IAP now.

Download and install the latest version of Wireshark (https://www.wireshark.org/) on a separate management machine. It is best that machine is wired, because the packets must be streamed from the IAP to the management machine running wireshark. Make sure the management machine does not have a firewall that blocks port UDP 5555

*Things to configure in Wireshark:

Go to Analyse > Decode As:

You should see a blank list. Click on Add and select Aruba ERM, Value 0, Integer, base 10 and current is ARUBA ERM PCAP (type 0)

0			📕 Wire	shark · Decode As	
Field	Value	Туре	Default	Current	
Aruba ERM Type	0	Integer, base 10	(none)	ARUBA ERM PCAP (Type 0)	

SSH into the IAP when it reboots. *Packet captures on Instant can only be initiated on the commandline.

Type "show pcap" to make sure that no other packet captures are already taking place:



If a pcap is running type pcap stop <bssid> <pcap-id>

The packet capture command takes a bssid parameter, so even if you turn a radio into an AM you need to find that BSSID to start the packet capture:

Type "show ap monitor status | begin WLAN" to get the BSSID:

IAF-135-Test# show ap monitor status begin WLAN WLAN Interface										
bssid			probe-type	phy-type		channel	pkts	max-ap-cl-delay	max-sta-cl-delay	last-reinit-time
d8:c7:c8:40:10:d0	enable	enable	sap	80211a-HT-20	tuned		208744	supp		
d8:c7:c8:40:10:c0	enable	enable		80211b/g-HT-40			52622	supp		

In this case on the 802.11b/g radio the bssid is d8:c7:c8:40:10:co

Before I start my pcap, I need to start Wireshark Capture on my management PC so that I can see the stream. Start capturing on the interface that the management PC is plugged into (Local). Then I would type WLAN and press enter in the filter:

Capturing from Local Area Connection [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]						
<u>File Edit View Go Capture Analyze Statistics</u>	Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp					
● ● ◢ ■ ∠ ⊨ ≞ ≭ 2 < +	• • • • 7 生 🔲 🗐 🔍	Q. Q. 🖂 👹 🖾 🥵 % 🛄				
Filter: wlan	 Expression 	Clear Apply Save				
No. Time Source E	Destination Protocol Le	ength Info				
45965 57.6227730 ArubaNet_b6:5d:90	Broadcast 802.11	312 Beacon frame, SN=3231, FN=0, Flags=, BI=100[Malformed Packet]				
45966 57.6231620 ArubaNet_b6:5d:96 #	Broadcast 802.11	253 Beacon frame, SN=3186, FN=0, Flags=, BI=100, SSID=sys-tb2-veriwave[Malformed Packet]				
45967 57.6231770 ArubaNet_b6:5d:97 H	Broadcast 802.11	237 Beacon frame, SN=3185, FN=0, Flags=, BI=100, SSID=bcontract[Malformed Packet]				
45968 57.6260630 ArubaNet_b6:5d:98	Broadcast 802.11	254 Beacon frame, SN=3180, FN=0, Flags=, BI=100, SSID=sys-tb2-veriwave1[Malformed Packet]				
45969 57.6260630 ArubaNet_b6:5d:99	Broadcast 802.11	243 Beacon frame, SN=3179, FN=0, Flags=BI=100, SSID=sys-tb2-4meshpt[Malformed Packet]				
45970 57.6290780 ArubaNet_32:04:53	ArubaNet_02:04:10 802.11	227 Probe Response, SN=2521, FN=0, Flags=, BI=100, SSID=dotx-auth-surv[Malformed Packet]				
45971 57.6290790 ArubaNet_32:04:54	ArubaNet_02:04:10 802.11	226 Probe Response, SN=1382, FN=0, Flags=, BI=100, SSID=109-auth-surv[Malformed Packet]				
45972 57.6290800 ArubaNet_c0:b6:b2	Broadcast 802.11	233 Beacon frame, SN=697, FN=0, Flags=, BI=100, SSID=guest				
45973 57.6290800 ArubaNet_c0:b6:b3	Broadcast 802.11	235 Beacon frame, SN=688, FN=0, Flags= BI=100, SSID=AppleTV[Malformed Packet]				
45974 57.6290800 ArubaNet_c0:b6:b4	Broadcast 802.11	235 Beacon frame, SN=684, FN=0, Flags=, BI=100, SSID=ajaytls				

To start my pcap, I need to go back to my IAP commandline and type:

pcap start <bssid> <ip address of management station with wireshark> 5555 0 2048 <channel>

Where bssid = the bssid we got from the radio above

Ip address = ip address of the management station we installed wireshark on

5555 is the port that Wireshark is looking for the Aruba pcap traffic on

0 means we are doing traditional PCAP (1 is for omnipeek)

2048 is the max packet size

Channel is of course, the channel.

Troubleshooting:

To stop the packet capture, first find out if a pcap is running by typing "show pcap".