Ruckus AP Remote packet capture to Wireshark

This same procedure will allow you to capture not only from the Wireless interface, but also from the other interfaces Available on the AP.

Informational - nice to know before starting

```
rkscli: get wlanlist
name           status   type   wlanID   radioID  bssid
-----------------------------------------------------------------
svcp           up       AP     wlan0    0        2c:5d:93:30:5b:48
home           up       AP     wlan1    0        2c:5d:93:70:5b:48
rcks           up       AP     wlan2    0        2c:5d:93:b0:5b:48
mdfx           down     AP     wlan3    0        00:00:00:00:00:00
wlan4          down     AP     wlan4    0        00:00:00:00:00:00
wlan5          down     AP     wlan5    0        00:00:00:00:00:00
wlan6          down     AP     wlan6    0        00:00:00:00:00:00

wlan100        down     MON    wlan100  0        00:00:00:00:00:00
wlan32         up       AP     wlan32   1        2c:5d:93:30:5b:4c
wlan33         up       AP     wlan33   1        2c:5d:93:70:5b:4c
wlan34         up       AP     wlan34   1        2c:5d:93:b0:5b:4c
wlan35         down     AP     wlan35   1        00:00:00:00:00:00
wlan36         down     AP     wlan36   1        00:00:00:00:00:00

wlan57         down     AP     wlan57   1        00:00:00:00:00:00
wlan58         down     AP     wlan58   1        00:00:00:00:00:00
wlan101        down     MON    wlan101  1        00:00:00:00:00:00
OK
rkscli:
```

Command

Note: Monitor (see type column) Interface for 2.4GHz Radio

Note: Monitor (see type column) Interface for 5GHz Radio

Step 1 – AP

Turn streaming on

If you want to capture on 2.4GHz use wlan100
If you want to capture on 5GHz use wlan101

Turn Streaming off

```
rkscli: set capture wlan100 idle
OK
```

ssh into the AP (open remote terminal to AP)
2 commands, set capture, then see the interface status change

```
rkscli: set capture wlan100 stream
Capturing in 20 MHz channel BW
OK
rkscli: get wlanlist
name           status   type   wlanID   radioID  bssid
-----------------------------------------------------------------
svcp           up       AP     wlan0    0        2c:5d:93:30:5b:48
home           up       AP     wlan1    0        2c:5d:93:70:5b:48
rcks           up       AP     wlan2    0        2c:5d:93:b0:5b:48
mdfx           down     AP     wlan3    0        00:00:00:00:00:00
wlan4          down     AP     wlan4    0        00:00:00:00:00:00
wlan5          down     AP     wlan5    0        00:00:00:00:00:00
wlan6          down     AP     wlan6    0        00:00:00:00:00:00

wlan26         down     AP     wlan26   0        00:00:00:00:00:00
wlan100        up       MON    wlan100  0        00:00:00:00:00:00
wlan32         up       AP     wlan32   1        2c:5d:93:30:5b:4c
wlan33         up       AP     wlan33   1        2c:5d:93:70:5b:4c
wlan34         up       AP     wlan34   1        2c:5d:93:b0:5b:4c
wlan35         down     AP     wlan35   1        00:00:00:00:00:00

wlan57         down     AP     wlan57   1        00:00:00:00:00:00
wlan58         down     AP     wlan58   1        00:00:00:00:00:00
wlan101        down     MON    wlan101  1        00:00:00:00:00:00
OK
rkscli:
```

Command 1

Command 2

Note: Monitor (see type column) Interface for 2.4GHz Radio

Note: Monitor (see type column) Interface for 5GHz Radio

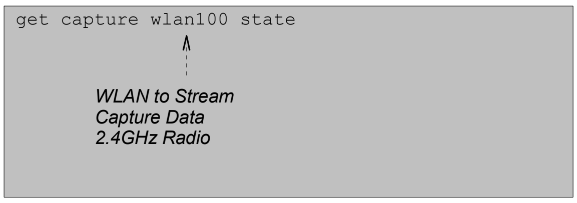
Step 2 – AP

Open interface for Wireshark to Connect

Still using AP ssh remote terminal

```
rkscli: get capture wlan100 state
wlan100: Packet Capture state: stream
OK
rkscli:
```

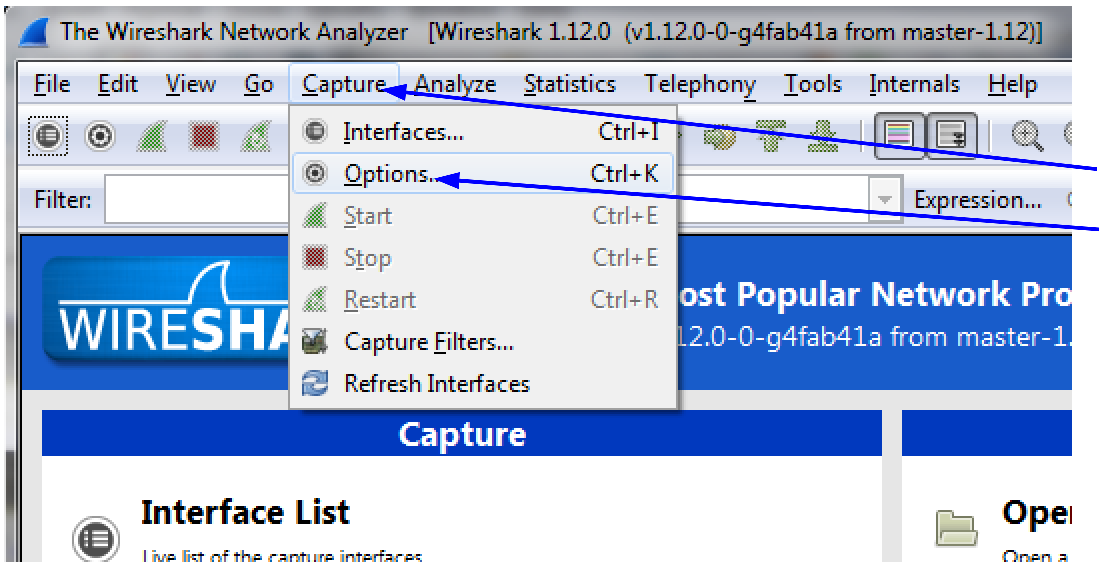
Command



Step 3 – Wireshark

Open Wireshark and configure to gather captures

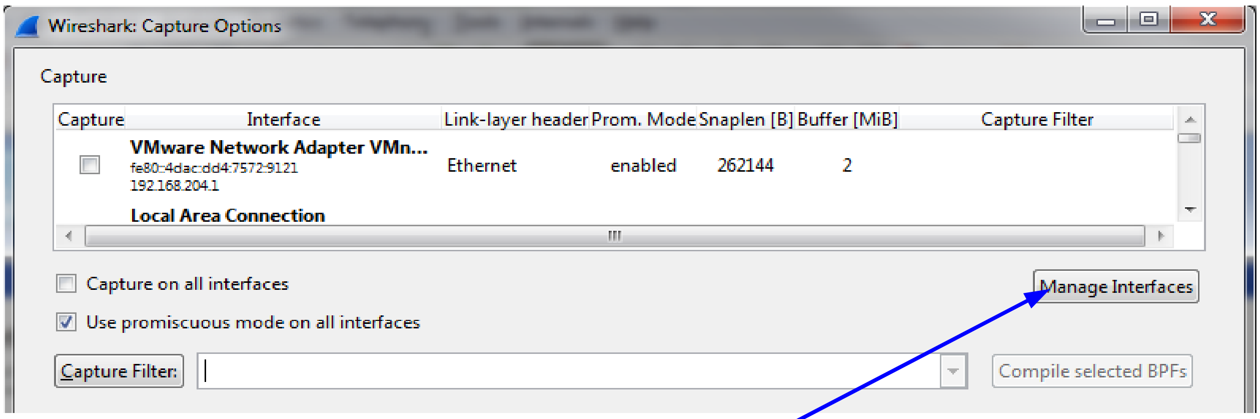
3a) Get into the “Options” menu to setup connection with AP [select “Capture” -> “Options”]


The Wireshark Network Analyzer [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces
WIRESHA
ost Popular Network Pro
12.0-0-g4fab41a from master-1.
Capture
Interface List
Live list of the capture interfaces
Ope
Open a

1-Click “Capture”

2-Click “Options”

3b) Open the Interfaces Screen to define remote capture AP [select “Manage Interfaces” button]



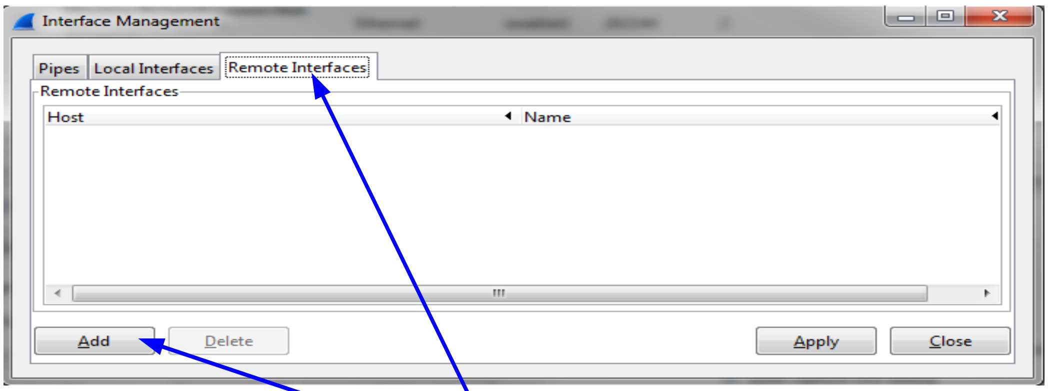
Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
□	**VMware Network Adapter VMn...** fe80::4dac:dd4:7572:9121 192.168.204.1	Ethernet	enabled	262144	2	
	Local Area Connection					

□ Capture on all interfaces

☑ Use promiscuous mode on all interfaces

1-Click “Manage Interfaces” Button

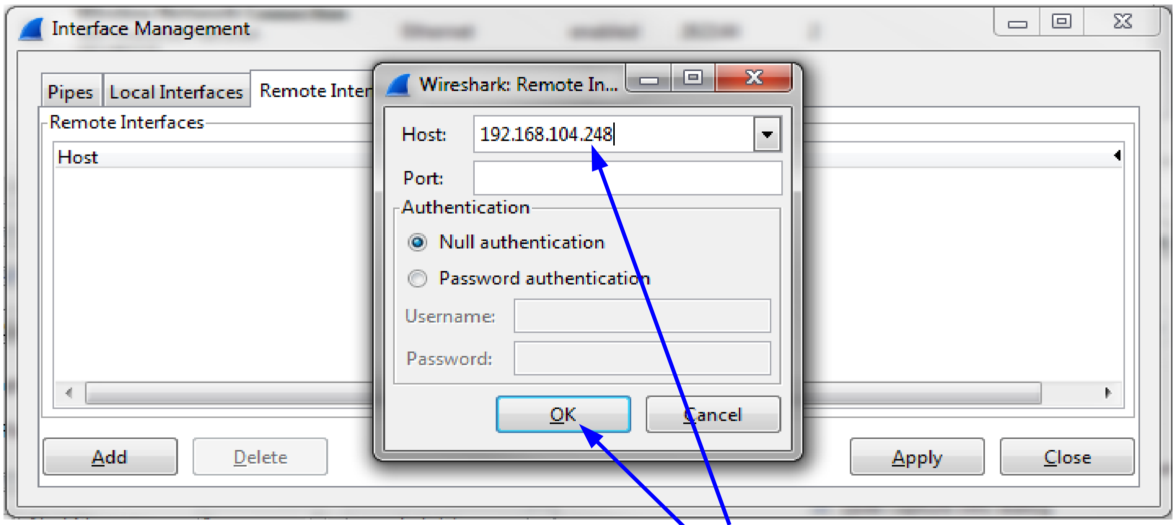
3c) Begin Add Remote interface [select “Remote Interfaces” Tab, Click “Add” button]



1-Click “Remote Interfaces” Tab

2-Click “Add”

3d) Add IP Address of Remote AP [enter IP Address of AP, click OK]



Host: 192.168.104.248

Port:

Authentication

● Null authentication

○ Password authentication

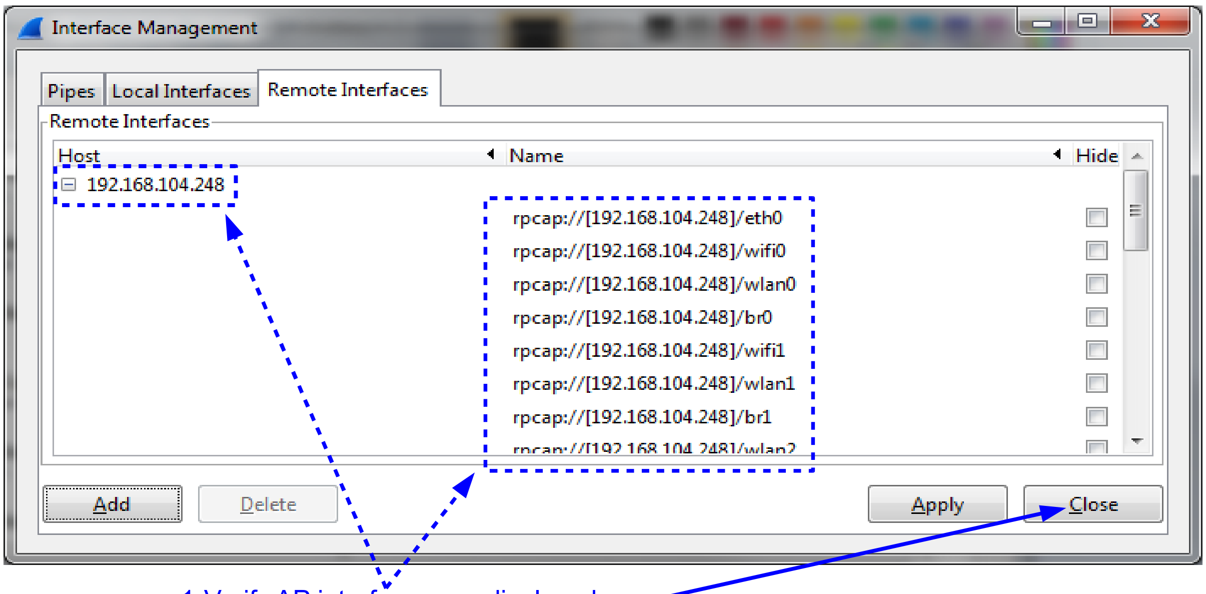
Username:

Password:

1-Enter IP Address of AP

2-Click “OK” Button

3e) Verify AP interfaces show up in Wireshark [you should see this window, click “Close” button]



Interface Management

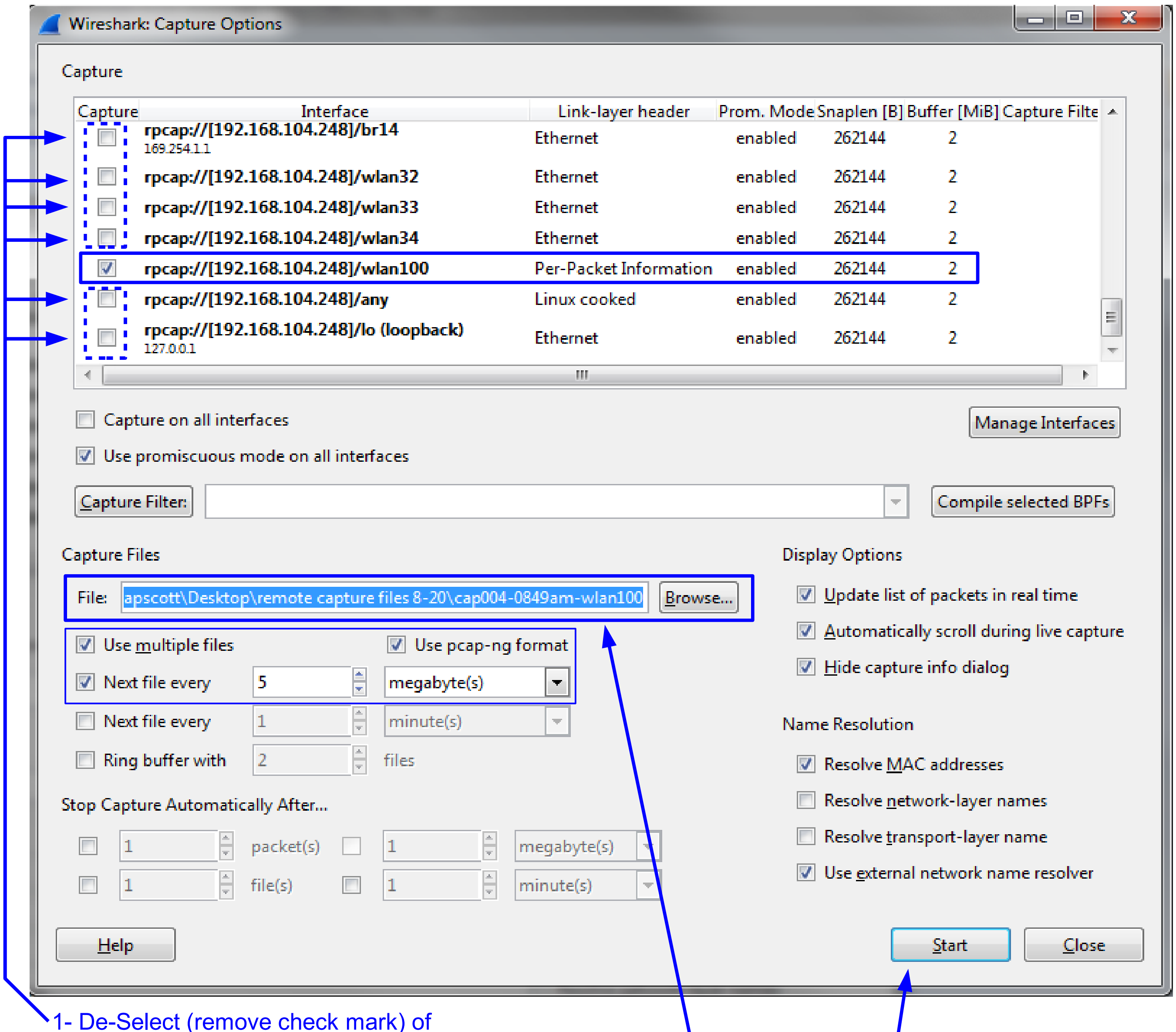
Pipes | Local Interfaces | Remote Interfaces

Remote Interfaces

Host	Name	Hide
⊟ 192.168.104.248		
	rpcap://[192.168.104.248]/eth0	□
	rpcap://[192.168.104.248]/wifi0	□
	rpcap://[192.168.104.248]/wlan0	□
	rpcap://[192.168.104.248]/br0	□
	rpcap://[192.168.104.248]/wifi1	□
	rpcap://[192.168.104.248]/wlan1	□
	rpcap://[192.168.104.248]/br1	□
	rpcap://[192.168.104.248]/wlan2	□

1-Verify AP interfaces are displayed
2-Click “Close” Button

3f) Select AP interface to use for Capture, Define File name for Capture Data, I use Multiple files
[un-checkmark the interfaces you dont want a capture from, Enter Capture file name, click Start Button]



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filte
□	rpcap://[192.168.104.248]/br14 169.254.1.1	Ethernet	enabled	262144	2	
□	rpcap://[192.168.104.248]/wlan32	Ethernet	enabled	262144	2	
□	rpcap://[192.168.104.248]/wlan33	Ethernet	enabled	262144	2	
□	rpcap://[192.168.104.248]/wlan34	Ethernet	enabled	262144	2	
☑	rpcap://[192.168.104.248]/wlan100	Per-Packet Information	enabled	262144	2	
□	rpcap://[192.168.104.248]/any	Linux cooked	enabled	262144	2	
□	rpcap://[192.168.104.248]/lo (loopback) 127.0.0.1	Ethernet	enabled	262144	2	

□ Capture on all interfaces

☑ Use promiscuous mode on all interfaces

Capture Filter:

Capture Files

File: apscott\Desktop\remote capture files 8-20\cap004-0849am-wlan100

☑ Use multiple files ☑ Use pcap-ng format

☑ Next file every 5 megabyte(s)

□ Next file every 1 minute(s)

□ Ring buffer with 2 files

Stop Capture Automatically After...

□ 1 packet(s) □ 1 megabyte(s)

□ 1 file(s) □ 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatically scroll during live capture

☑ Hide capture info dialog

Name Resolution

☑ Resolve MAC addresses

□ Resolve network-layer names

□ Resolve transport-layer name

☑ Use external network name resolver

1- De-Select (remove check mark) of interfaces you dont want

2- Set the File Name and Directory for Capture Data to be saved to

3- Click “Start” Button

Step 4 – AP

Disable Capture from AP

```
rkscli: set capture wlan100 idle
OK
```

Command