Wireshark Filters for 802.11 packet captures

- The filter syntax for the various header fields is shown in the following table:

802.11 Header Fields	
Either Source or Destination MAC Address	wlan.addr
Destination MAC Address	wlan.da
Source MAC Address	wlan.sa
Receiver Mac Address	wlan.ra
Transmitter MAC Address	wlan.ta
BSSID	wlan.bssid
Duration	wlan.duration

- The filter syntax for the Frame Control Subfields is shown in the following table:

Frame Control Subfields	
Frame Type	wlan.fc.type
Frame Subtype	wlan.fc.subtype
ToDS Flag	wlan.fc.tods
FromDS Flag	wlan.fc.fromds
Retry Flag	wlan.fc.retry
Protected Frame (WEP) Flag	wlan.fc.wep

- Wireshark makes it very convenient to analyze the 802.11 packet captures provided. Simply use the filter bar and enter a filter string specifying the exact frame types and subtypes of interest.

- The following table provides a convenient quick reference for the more common fields:

Frame Type/Subtype	Filter
Management Frames	**wlan.fc.type==0**
Association Request	wlan.fc.type_subtype==0
Association Response	wlan.fc.type_subtype==1
Ressociation Request	wlan.fc.type_subtype==2
Ressociation Response	wlan.fc.type_subtype==3
Probe Request	wlan.fc.type_subtype==4
Probe Response	wlan.fc.type_subtype==5
Beacon	wlan.fc.type_subtype==8
ATIM	wlan.fc.type_subtype==9
Disassociate	wlan.fc.type_subtype==10
Authentication	wlan.fc.type_subtype==11
Deauthentication	wlan.fc.type_subtype==12
Control Frames	**wlan.fc.type==1**
Power-Save Poll	wlan.fc.type_subtype==26
Request To Send - RTS	wlan.fc.type_subtype==27
Clear To Send - CTS	wlan.fc.type_subtype==28
Acknowledgement -ACK	wlan.fc.type_subtype==29
Data Frames	**wlan.fc.type==2**
NULL Data	wlan.fc.type_subtype==36