

A-7 Details: True

The *cfilters* file can be shared with other Wireshark users by simply copying the file into another host's personal preferences folder. If you are sharing an entire profile that contains special capture filters, simply copy the entire *profiles* directory to the other Wireshark system. (If you want the details on how Wireshark creates files when you build profiles, see Chapter 11 of the Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide book.) The *cfilters* file is just a simple text file and has no link to the local system configuration so it can be moved about freely.

❖ **Chapter 3: Capture Traffic****A-8 Details: C**

Promiscuous mode operation enables an interface to capture packets that are sent to any MAC addresses. If promiscuous mode is disabled, you will only capture traffic that would normally be picked up by the adapter and processed. This includes broadcast packets, multicast packets and packets to your own MAC address. To be an effective analyst, you will want to keep this setting enabled. If, however, you simply want to quickly capture all traffic to/from your own system without setting up a capture filter, you can use this setting. Promiscuous mode does not enable a WLAN adapter to capture packets regardless of the SSID value—that is monitor mode. Promiscuous mode does not simply enable an interface to capture gratuitous ARP request and response packets—it does much more. Promiscuous mode does not enable an interface to capture packets addressed to broadcast and multicast addresses—you already have that capability without promiscuous mode enabled.

❖ **Chapter 3: Capture Traffic****A-9 Details: True**

AirPcap adapters can be used to expand Wireshark's ability to capture wireless network traffic in a Windows environment. AirPcap adapters were created by CACE Technologies (the company where Gerald Combs, creator of Wireshark, works). The AirPcap adapters can go into monitor mode (not join any SSID in order to capture traffic on all WLANs seen) and the adapters will pass up the 802.11 management, control and data frames. In addition, AirPcap adapters can place a Radiotap or PPI header in front of the 802.11 header. These additional headers provide channel and signal information at the moment the packet was captured. You may be able to capture WLAN traffic using your native adapter, but there is a good chance that your 802.11 header will be replaced with an Ethernet II header. The adapter strips the 802.11 header off the packet and Wireshark puts in a