applications such as web browsers. The *hosts* file kept in the Wireshark global or personal preferences directory is referenced first before Wireshark performs network name resolution (if Wireshark is configured to perform network name resolution).

❖ **Chapter 5: Define Global and Personal Preferences**

A-27 Details: B

Based on the Capture Options window shown, Wireshark will scroll to display the most recent packet captured. This may be surprisingly useless on very busy networks as packets fly by too quickly to watch. This feature is better suited to a capture on a low packet rate network or when you are using a capture filter to reduce the number of packets captured or a display filter to reduce the number of packets shown. In the Capture Options window shown, Wireshark is not configured to resolve IP addresses to host names (**Enable network name resolution** is disabled) or resolve OUI values for all MAC addresses (**Enable MAC name resolution** is disabled). The configuration shown does not indicate Wireshark is set to automatically stop capturing packets after two files have been saved (**Stop capture after** is not defined).

❖ **Chapter 3: Capture Traffic**

A-28 Details: True

Display filters applied to a trace file before opening the **Protocol Hierarchy Statistics** window are automatically applied to the results displayed. This is a handy feature if you are focusing on the various protocols/applications transmitted to or from a particular host—you can apply an `ip.addr` display filter before opening the Protocol Hierarchies window.

❖ **Chapter 2: Introduction to Wireshark**

A-29 Details: A

The capture filter highlighted in the image is illogical as the title indicates the purpose is to filter out ARP and DNS packets. The filter is configured with the `or` operator, however. Packets only need to match one side of the `or` operator—both ARP and DNS packets would be displayed. For example, if this capture filter is applied to a DNS packet it would be displayed because that packet is not an ARP packet. In general, this capture filter won't have any effect on the network traffic. The correct filter would be `not arp and not dns`. Wireshark includes a number of sample capture filters that show how to filter out various types of traffic.

❖ **Chapter 4: Create and Apply Capture Filters**