Hands-on Exercise One Solution

a) 131.247.95.216 is the source address.

b) It is www.google.com located at 64.233.161.99, 64.233.161.104, or 64.233.161.147

   This information can be found in the payload of the second packet. In the middle Ethereal window open the Domain Name System, then open the Answers line.

c) The client is requesting a conversation with the web server. It negotiates the connection and agrees to the sequence numbers that will be used for acknowledgement of messages. This is a three-way handshake.

d) In frame six, the browser requests a web page. In frame seven, the server acknowledges the receipt of the request.

e) Provided as a comment, not an exercise question.

f) This is the actual web page sent in response to the original HTTP get statement. It is google's front page. The page is segmented into two packets (nine and ten), and it must be reassembled to get the full page.

g) This is the acknowledgement from the client browser that it received the web page.

h) The web page that is received in packets nine and ten only contains the text and layout instructions for the web page. Once the browser interprets the web page, it sees that it needs to get an image called logo.gif in order to complete rendering the web page. This packet is the request for the logo.

i) This is the logo being sent to the browser by the server. The set of packets also includes a number of acknowledgements sent by the client back to the server. It takes this many packets because of the size of the logo file – it must be sent as separate packets that are then reassembled into the gif file.

j) The browser requests the favicon.ico for the page. The server ack's the request, and send back the icon in packets 24 and 25. In packet 26 the client ack's the receipt of the favicon.ico.

k) This set of packets came from the user typing in www.google.com.