1. How many packets (frames) are there in this capture?

A: There are 499 packets, or frames, in this capture.

2. Choose the first frame in the top pane. Expand the Internet Protocol triangle of this frame in the middle pane.

a. What are the source and destination addresses of this packet?

A: The source address is 10.1.3.143 and the destination address is 10.1.6.18.

b. To what entities do these numbers refer?

A: These numbers represent Internet Protocol (IP) addresses of computers on a private network.

3. Expand the Transmission Control Protocol triangle of the packet.

a. What are the source and destination ports of this packet?

A: The source port is 32803 and the destination port is 1720.

b. To what entities do these numbers refer?

A. These numbers represent the port numbers being used to implement a connection by one or more applications.

4. Note that wireshark is smart enough to "know" which ports are typically used by internet applications. What service is the host at IP 10.1.3.143 trying to access on the host with IP 10.1.6.18?

A: The host is attempting to access the H.323 Video Conferencing service as indicated by the use of the TCP port 1720 to initiate a call with the H.225 protocol for call control, which is followed by utilizing a dynamic TCP port, 1232 in this case, to access the H.245 protocol for capabilities exchange and change control, and then two dynamic UDP ports for each type of media that was negotiated for the call are opened, specifically ports 2006 and 5000.

5. Read this discussion excerpted from the previous hint and answer the questions that follow as best you can:

H.323 uses a single fixed TCP port (1720) to start a call using the H.225 protocol (defined by H.323 suite) for call control. Once that protocol is complete, it then uses a dynamic TCP port for the H.245 protocol (also defined by the H.323 suite) for capabilities exchange (caps exchange) and channel control. Finally, it opens up two dynamic UDP ports for each type of media that was negotiated for the call (audio, video, far-end camera control, etc.). This first port carries the RTP protocol data (defined by the H.225 specification) and the second one carries the RTCP data (defined by the H.225 specification).

a) Which frame first accesses port 1720 and, hence, initiates the exchange?
A: Frame 1

b) At which frame do the parties shift to using another pair of ports (for the H.245 protocol)?
A: Frame 12 is when the new pair of ports are first accessed, but Frame 15 is when they are starting to be used for the H.245 protocol.

c) At which frame do they begin the real-time protocol (RTP) specified by H.225?
A: Frame 34

Questions - Part 2

1. Frame 1 - client is requesting an IP address. Expand the Bootstrap Protocol.
   a. What does DHCP stand for?
   A: Dynamic Host Configuration Protocol.

   b. What do you think DHCP Discover means?
   A: DHCP Discover is a host that is trying to locate a valid DHCP server in order to make use of a specific local IP address.

2. Frame 2 - expand the Bootstrap Protocol.
   a. What do you think DHCP Offer means?
   A: DHCP Offer indicates an offered valid DHCP server along with its available local IP addresses. Essentially, DHCP Offer lists network information for the offered DHCP server as a result of a DHCP Discover request.

3. Frame 3 - expand the Bootstrap Protocol.
   a. What has the "client" requested of the DHCP server?
   A: The client requested a local IP address from the offered DHCP server network.

4. Frame 4 - The client now has an IP address.
   a. What is this address?
   A: The client now has the IP address 192.168.0.10.