Wireshark HTTP and DNS Labs Addendum

Tom Kelliher, CS 325

Feb. 21, 2011

Reminder: When printing packet data, choose the "Selected packet only" radio button. The default is to print "All packets," which is usually overkill and wastes paper.

Capturing Live Data

1. To capture live network data, you must run Wireshark as root. Follow these steps:
   (a) Open a command-line shell: `Applications` → `Accessories` → `Terminal`.
   (b) Enter the command:
   ```
   wireshark &
   ```
   (c) Wireshark will run in the background, popping up its main window. A small pop-up warning dialog box might also pop up. If necessary, dismiss it.
2. To start a packet capture session, do the following:
   (a) Open `Capture` → `Interfaces`. Click the `Options` button to the right of the `eth0` device.
   (b) **Heed the following if you're running Wireshark remotely.** The Capture Options might show a Capture Filter similar to:
   ```
   not ip host bluebird.goucher.edu
   ```
   Replace that Capture Filter with:
   ```
   not tcp port 22
   ```
   This will filter the SSH packets used by NX during your remote session.
   (c) Click the `Start` button to start the capture.
   Click the `Stop` button on the main Wireshark window to stop the capture.

HTTP Lab Addendum

Turn in your responses to the questions asked in the lab.

1. Section 2: If you don't get the expected response from the URL given in this section, try `http://phoenix.goucher.edu/`.

2. Section 4: One of the image links within the URL given in this section is broken. Instead try `http://phoenix.goucher.edu/~kelliher/s2011/cs325/images.html`.

3. Section 5: Another option is to try
   `http://phoenix.goucher.edu/~kelliher/s2011/cs325/files`.

   If you look carefully, you notice that Wireshark does the base64 decoding for you.

DNS Lab Addendum

Turn in your responses to the questions asked in the lab.

1. `nslookup` is available from the Linux command line shell. It's also available from the command line shell in Windows 7. (But why would you want to use 7 when you can use Linux?)

2. Section 2: Under Linux run

   ```
   /sbin/ifconfig eth0
   ```

   from the shell.

3. Section 3: Merlin doesn't use a local DNS cache, so there's nothing to clear.

   You can determine the IP addresses of the DNS servers in use on a Linux system by typing

   ```
   cat /etc/resolv.conf
   ```

   from the shell.