**Project 1:**

**Sniffing for Passwords with Wireshark**

**What You Need for This Project**

* A computer with Internet access. You need administrator privileges.
* I wrote the instructions with Windows 7

**Installing the Wireshark Packet Sniffer**

**$sudo apt-get install wireshark**

**To run wireshark**

**$sudo wireshark**

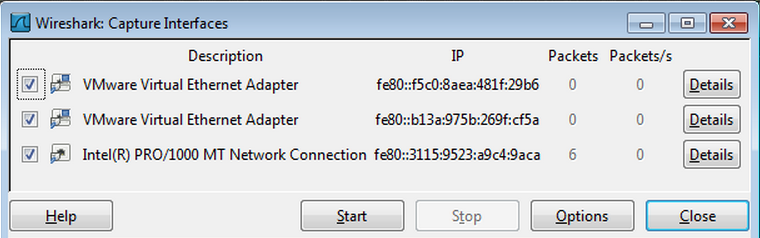
**Starting a Packet Capture**

Click **Start**, **Wireshark**.

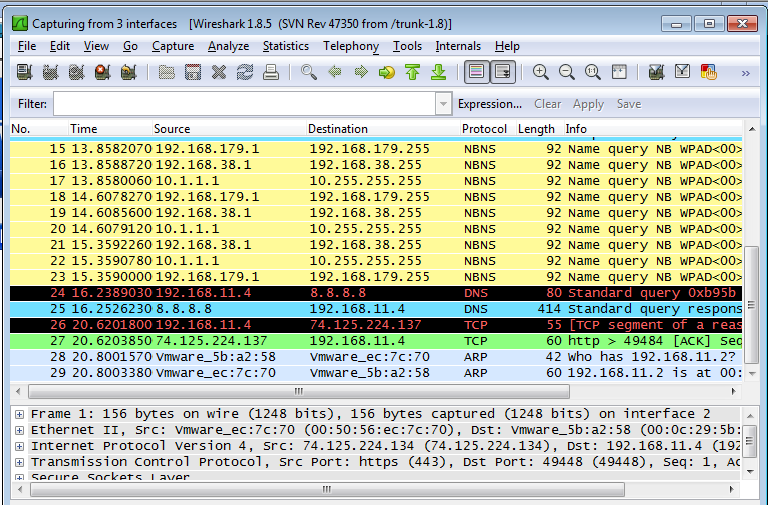
In Wireshark, on the left side, click "**Interface List**".

In the "Wireshark: Capture Interfaces" box, check all the interfaces, as shown below.

Click the **Start** button.



You should see packets being captured and scrolling by, as shown below on this page. Every packet sent from or to your machine is shown here. But it shows a lot more information than you usually want to know.

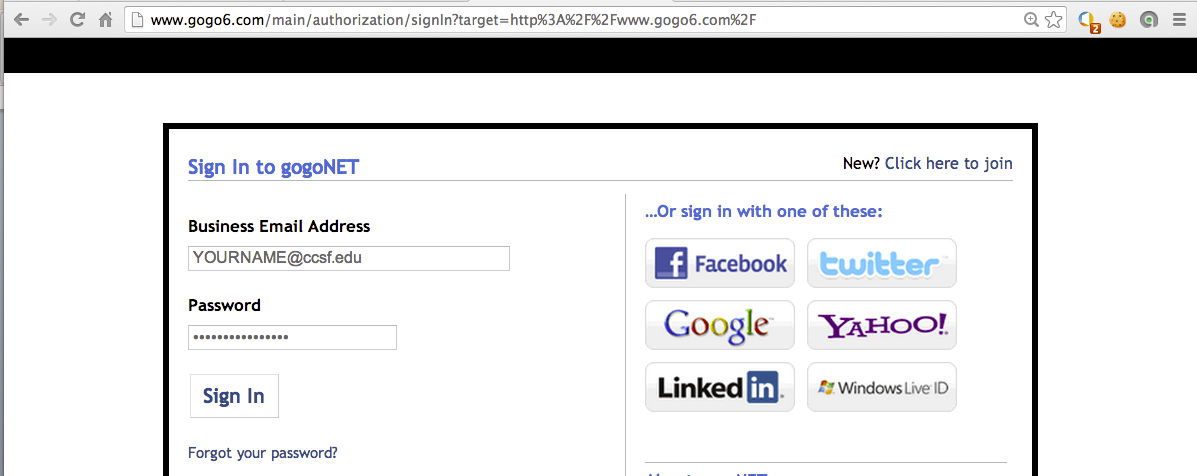


**Sending a Test Password to gogoNET**

Open a Web browser and go to [gogo6.com](http://www.gogo6.com/) (or abcnews.go.com) (or sbihmkgp.com/login)

On the top right of the screen, click "**Sign In**".

Enter a Username of **YOURNAME@ccsf.edu** (using your own name, not the literal string "YOURNAME") and a Password of **topsecretpassword**, as shown below:



Click the "**Sign In**" button. If you see a message asking whether to remember the password, click "**Not Now**".

You see an error message from gogoNET saying the login failed.

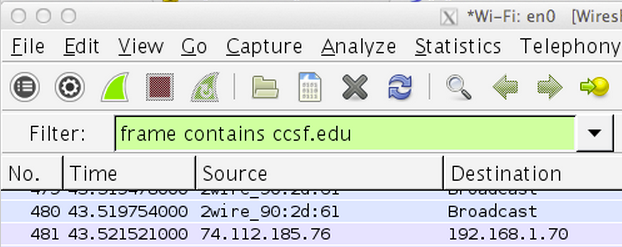
That doesn't matter--the point of this project is to see how the password was sent to gogoNET.

In the Wireshark window, box, click **Capture**, **Stop**.

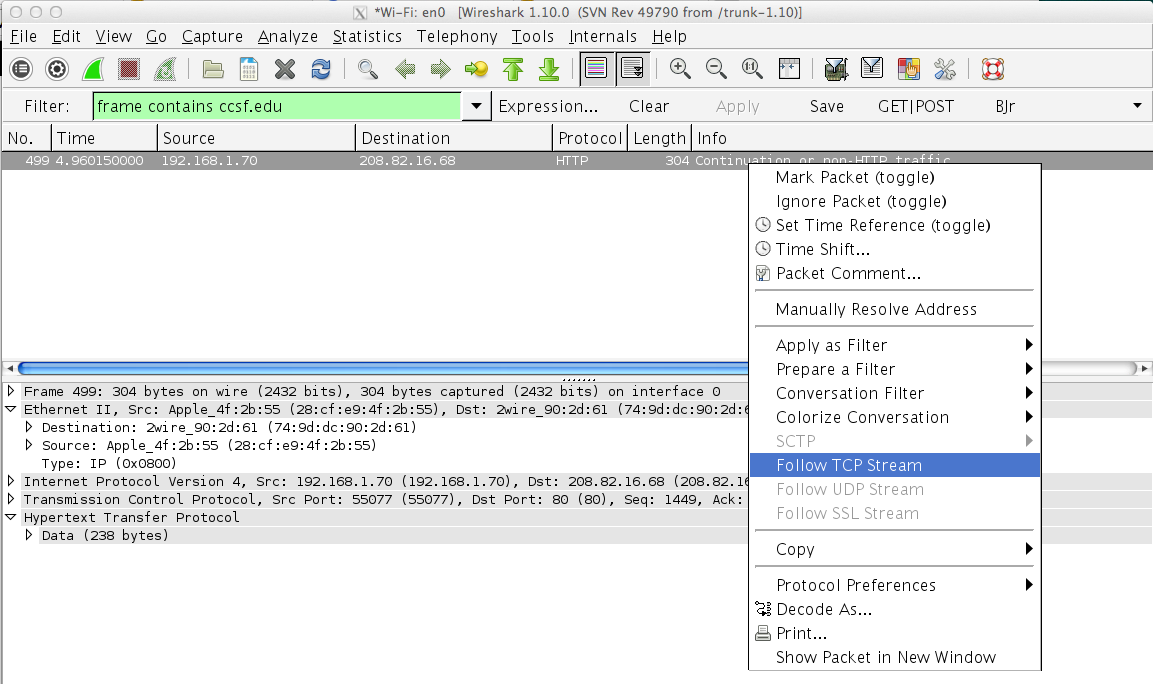
**Observing the Password in Wireshark**

In the Wireshark window, box, in the Filter bar,type this filter, as shown below:

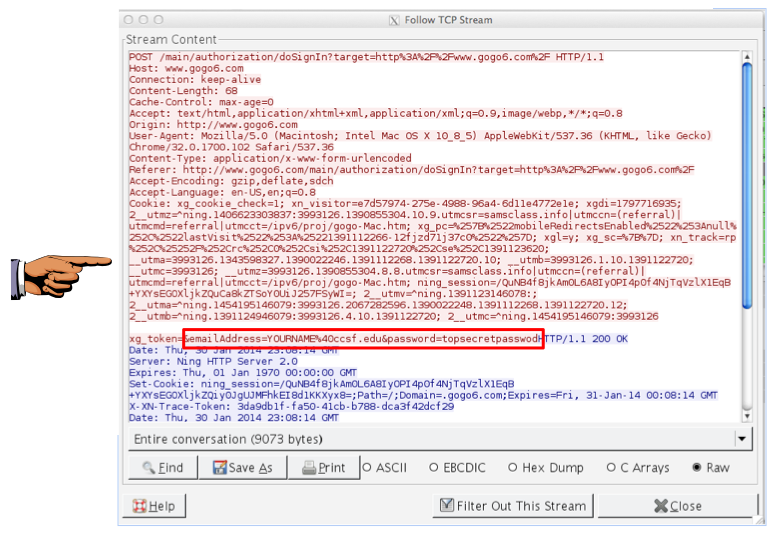
**frame contains ccsf.edu**



Wireshark shows an HTTP packet containing the text. In the upper pane of Wireshark, right-click the HTTP packet and click "**Follow TCP Stream**", as shown below.



Expand the "Follow TCP Stream" box so that you can see **YOURNAME** and the password of **topsecretpassword**, as shown below.



**Saving a Screen Image**

Make sure your screen shows these required items in the captured packet:

* Your Name
* The captured password "topsecretpassword"

Press **Ctrl+Alt** to release the mouse from the Virtual Machine.

Press the PrintScrn key in the upper-right portion of the keyboard. That will copy the whole desktop to the clipboard.

**YOU MUST SUBMIT AN IMAGE OF THE WHOLE DESKTOP TO GET FULL CREDIT!**

Open Paint and paste in the image.

Save the image with the filename "**Your Name Proj 3**". Use your real name, not the literal text "Your Name".

**Starting Another Packet Capture**

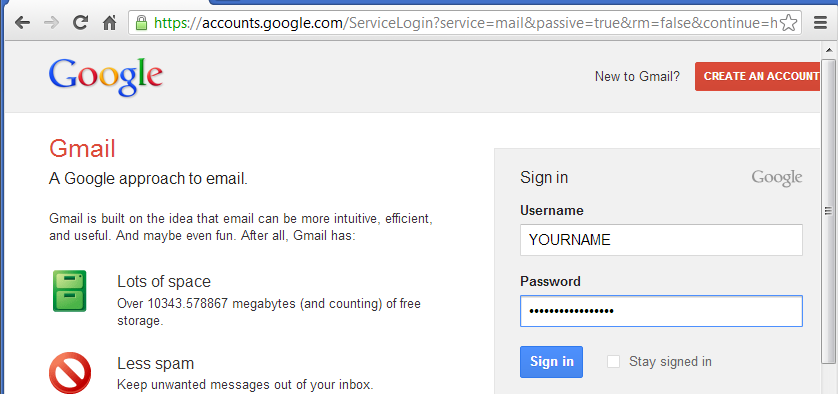
From the Wireshark menu bar, click **Capture**, **Start**. A bob pops up asking "Do you want to save the captured packets before starting a new capture?" Click "**Continue without saving**".

**Using a Secure Password Transmission**

In a Web browser, go to [http://gmail.com](https://gmail.com/)

Enter a Username of **YOURNAME** (using your own name, not the literal string "YOURNAME", and a Password of **topsecretpassword**, as shown below.

Click the "**Sign in**" button.



Gmail will reject the credentials, just like gogoNET did.

In the Wireshark window, box, click Capture, Stop.

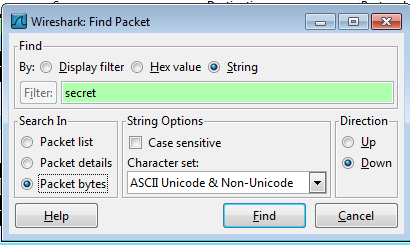
**Searching for the Password in Wireshark**

In the Wireshark window, box, click **Edit**, "**Find Packet**".

In the "Wireshark: Find Packet" box, click the **String** button. Enter a search string of **secret**, as shown below.

In the "Search In" section, click "**Packet bytes**".

Click **Find**.



A message appears briefly in the status bar at the bottom of the Wireshark window, saying "No packet contained that string", as shown below.

The password cannot be found because Gmail encrypts it before transmitting it.

