

Lab 2: Capturing and Understanding Network Packets (Precursor to Investigating Snort and IDSCenter)

Due: 9/16/09 in class

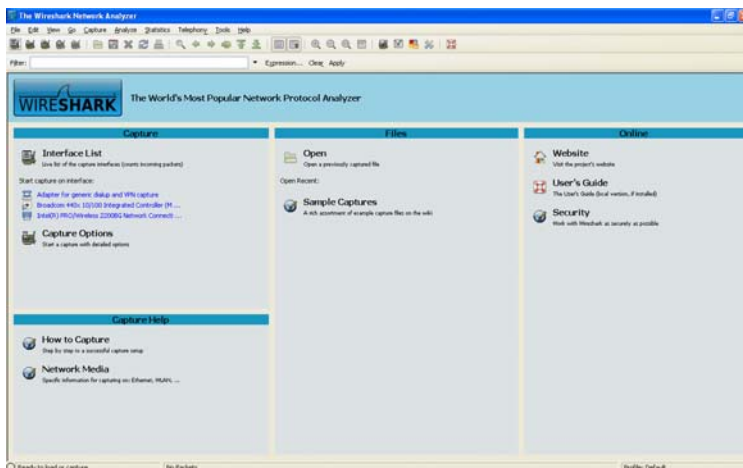
IDSs are composed of 3 main components: the **sensor** (collection of packets), the output of which is fed into the **analyzer** and the **user interface**.

Objectives - to:

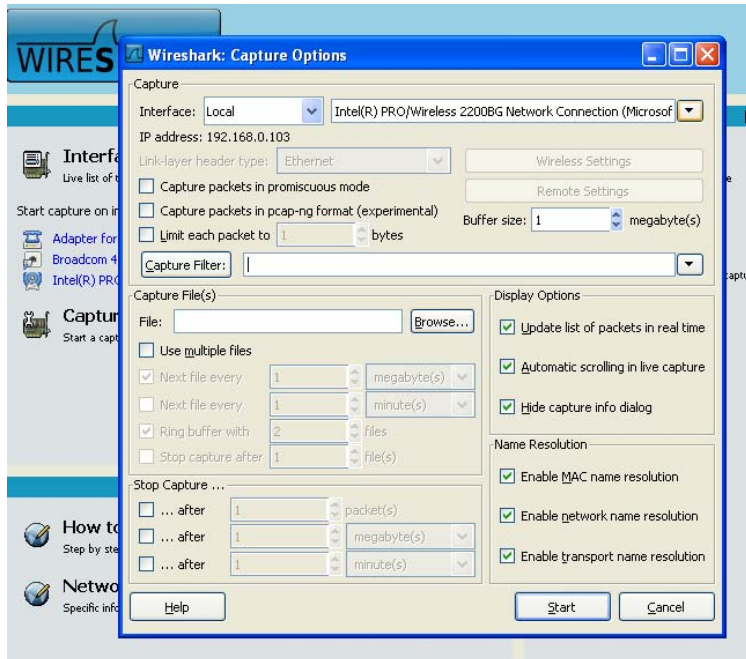
1. gauge an understanding of the types of information contained in packets, including protocols and IP addresses related to secure sites. This is in preparation for working with IDSs like Snort, in conjunction with IDSCenter, we will use Wireshark. Packet information such as these are fed into IDSs.
2. investigate protocols and procedures related to sites that require specific security measures (mail login and shopping carts)
3. level the field for those who are already familiar with network protocols and those who are not

Prelab Activities: familiarize yourself with Wireshark

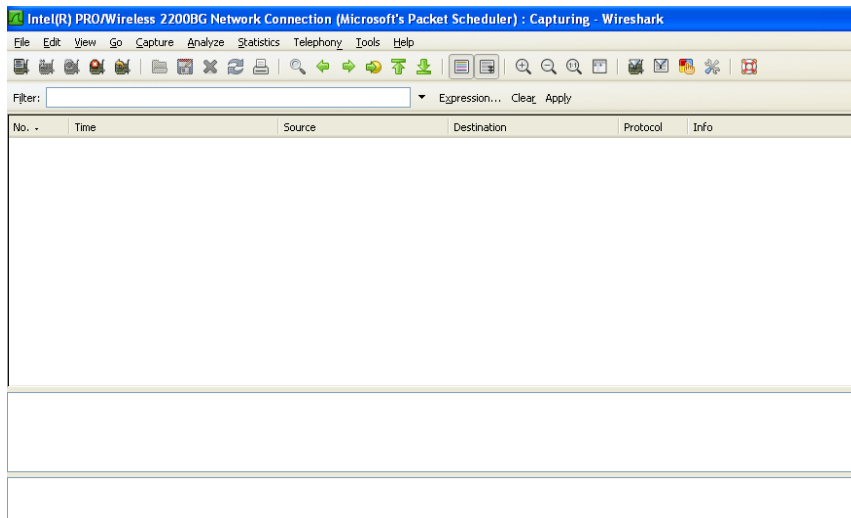
1. Close all browsers (including IM, email, Twitter, FB!)



2. Open up Wireshark and click on "Capture Options."



3. Your workstation may have several interfaces. Pick “Local” and then try the different interfaces to see which packet traffic Wireshark is picking up. Note: you may need to uncheck “capture packets in promiscuous mode” option.



4. At this screen, place your mouse over each of the icons on the tool bar to familiarize yourself with Wireshark. For example the 3rd icon is “start a new live capture”. Click on that and you should see some packet activity (you may have to wait about 30 seconds). The 4th icon “stops” the capture of packets. Note what do the green arrows do. How about the magnifying glass?
5. Once packets have been captured, double click on random lines to see the types of details available – you will need this for the exercises below.

Lab

Part A getting to know Wireshark - 7 points

1. Click on “start a new live capture” and note initial activity.
2. Click on the green arrow that finds the first packet.
3. Doubleclick on the first line.

4. Without using 'ipconfig', what is the IP address of your machine?

5. What is the first protocol that is visible? _____
6. On what port (shown in brackets)? _____
7. Open up any browser and go to 'cs.millersville.edu'
8. After 30 seconds, click on "stop the running live capture" icon
9. Click on the "find a packet" icon
10. Check the "String" button
11. Type 'cs.millersville.edu' and click on 'Find.'
12. Notice the highlighted line. What is the IP address for this server?

13. What is another visible protocol? _____
14. Doubleclick on this protocol to find on what port it is found _____
15. Attach a screen shot of your current screen (write your name and mark it as A 15)

Part B checking email (HTTPS) – 5 points

1. Go to 'File,' then, 'Quit,' and 'Quit without saving.'
2. Start a new live capture
3. Open a new browser and go to Yahoo! mail:
https://login.yahoo.com/config/login_verify2?&.src=ym
4. Type in some made-up username (e.g. nazlinazli@yahoo.com) and some made-up password
5. Go back to the Wireshark screen and search for 'https' – review Part A for this search function
6. What is the IP address of the Yahoo server you accessed? _____
7. On what port is https found? _____
8. Notice that there are additional IP addresses – look at the detailed logs to determine why Wireshark is capturing packet from those addresses

9. Stop capture
10. Attach a screen shot of your current screen (write your name and mark it as B 10)

Part C buying/ selling/ cc info (SSL) - 3 points

1. Start a new live capture (Capture/ Restart from the toolbar)
2. Go to Amazon.com and pretend to buy a Kindle, i.e. "proceed to checkout"
3. pretend you are a returning customer – make-up and password and sign in
4. Go back to Wireshark and search for 'client key exchange' – be sure to check the "packet details" box
5. Once you have found the line with the 'client key exchange', double click for details.
6. What is the IP address of this particular Amazon server? _____
7. What is TLS? _____
8. Maximize the 'client key exchange' detail screen and attach a screen shot of your current screen (write your name and mark it as C 8)

Total: 15 Points