


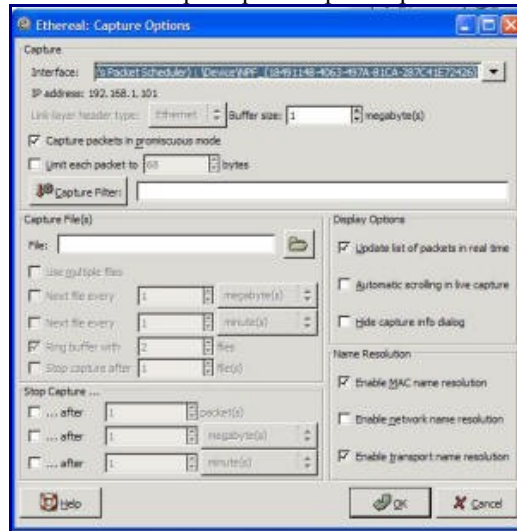
Step 1

[Install Ethereal](#)

Step 2
Once its installed, start up the program.

Step 3
Click on the Start New Capture Button 

Step 4
Once you have clicked on this it should open up the caption options dialog box that looks like this:



Step 5
In the dialog box click on interface and change this to your Ethernet card. (Hopefully everyone who is reading knows that you have to be directly connected to the modem, no firewall, and no router.)

Step 6
Based on the scans that I run I allocate 4mb to buffer which is on the second option. Then I make sure that capture in promiscuous mode is checked and that Limit Each Packet is **unchecked**.

Step 7
Where it says Capture Filter insert "udp"

Step 8
Go do your desktop. Once you are at your desktop right-click and go down to New, then over to text document.

Step 9
Now go back to Ethereal, and the Capture Options dialog box. Here go to where it says capture file. Click on Browse and go to the new file that you just created on your desktop called New Text Document.txt then click open and it will take you back to the Capture options dialog box.

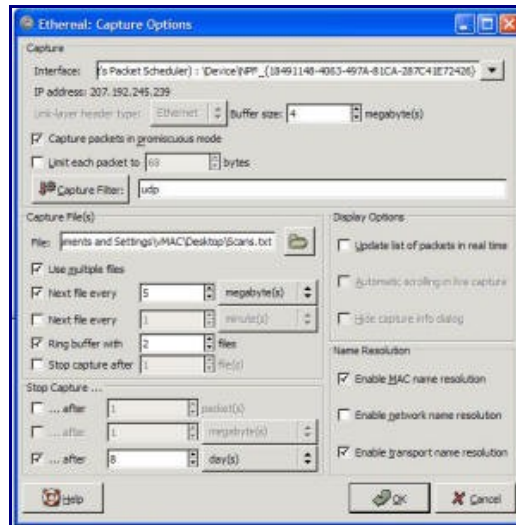
Step 10
Check use multiple files and then underneath check where it says "next file every" and change it to "5" mb. (This is what I do so that I don't have a 50mb text file, this is totally optional you don't have to do Multiple files if you don't want to.)

Step 11
Uncheck everything that is in the Display Options section of the dialog box. (If you know what you are doing and you are looking for a quick fix then you can check play around with these options. This is outside the scope of a basic tutorial so

play if you want.)

Step 12

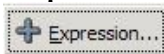
Under Name Resolution make sure that MAC address is **checked** and transport name is **checked** when you are done it should look like this



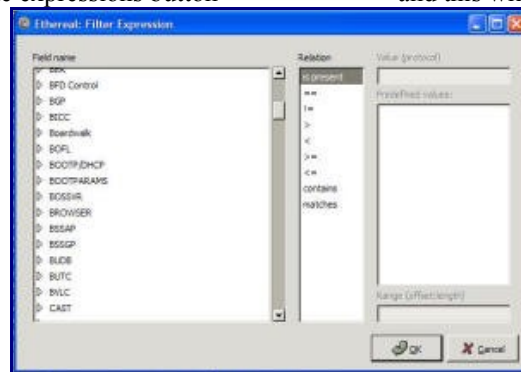
Step 13

Press OK on the dialog box and it will start capturing the files. Let it run for as long as you can. I wouldn't turn it off until after it has received over 3,000 packets but you can whenever you so choose if you are in a rush. After it has reached your desired packet level then press STOP. It will then load the text files into the Ethereal browser.

Step 14



Once it opens up click on the expressions button and this will open up the filter dialog box:

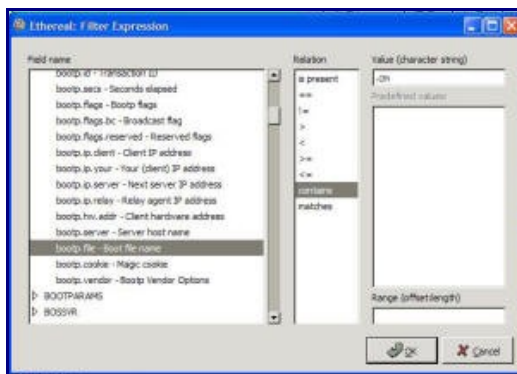


Step 15

Click on the arrow next to BOOTP/DHCP protocol in the Field Name section then go down and click on the "bootp.file - Boot File Name" option.

Step 16

Then in the Relation field click on Contains, then in the Value field type in .cm. If you have followed this tutorial completely your screen should look something like this:



If it does press OK.

Step 17

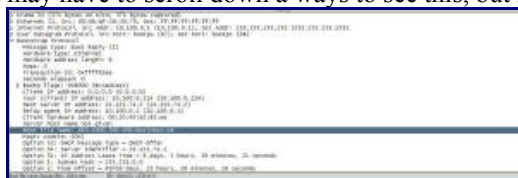


Now it will take you back to the Main screen. Click on Apply button which is to the right of the Expression button that you just pressed. It will then get rid of any packets that do not contain .cm which is the typical config file name. Now click on one of the packets on the top half of the screen which will bring up some information on the bottom half of the screen. Then in the bottom field click on the arrow next to Bootstrap Protocol. It should then look like this:



Step 18

Then look for a item name "boot file name" and it will show you what the name to your config file is. Also if you are looking for your TFTP server then it is under the "Server Identifier" section of the BOOTSTRAP information. You can see this on my picture below. You may have to scroll down a ways to see this, but it will look something like this:



Step 19

If when you press Apply no packets appear, and you have a substantial amount of packets, then up at the top in the field next to Filter erase where it says ".cm" and type in ".bin" then hit APPLY. If this still does not show any packets then type in ".cfg" and hit APPLY. If this still doesn't bring up any packets then type in ".md5" and hit APPLY.

Step 20

If you do all of these things and you don't have any packets then your ISP is setup very different or you aren't doing something correct. Go back through the process and try it again, maybe you need more packets collected before you can start to try and filter.

Step 21

Remember that the longer you sniff the better your results will be, if you just want to sniff for 5 minutes then you probably won't find anything. Typical leases for an ISP are 7 days. So the best bet in finding a good config file is to let this program run for 8 days straight this way all the computers will have asked for a renewal from the DHCP server and thus all the available configs used on your node will be within the packets.