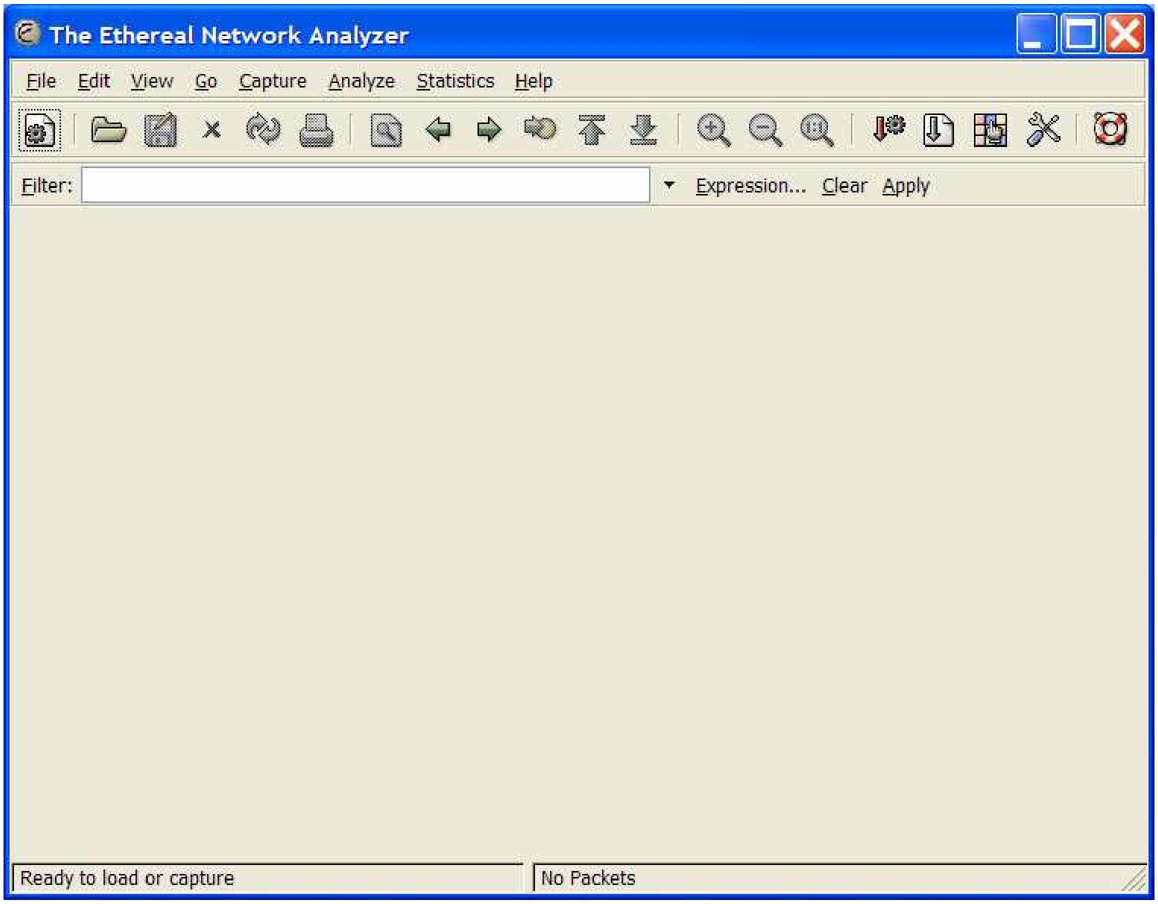
Laboratory 1

Software on your laptop

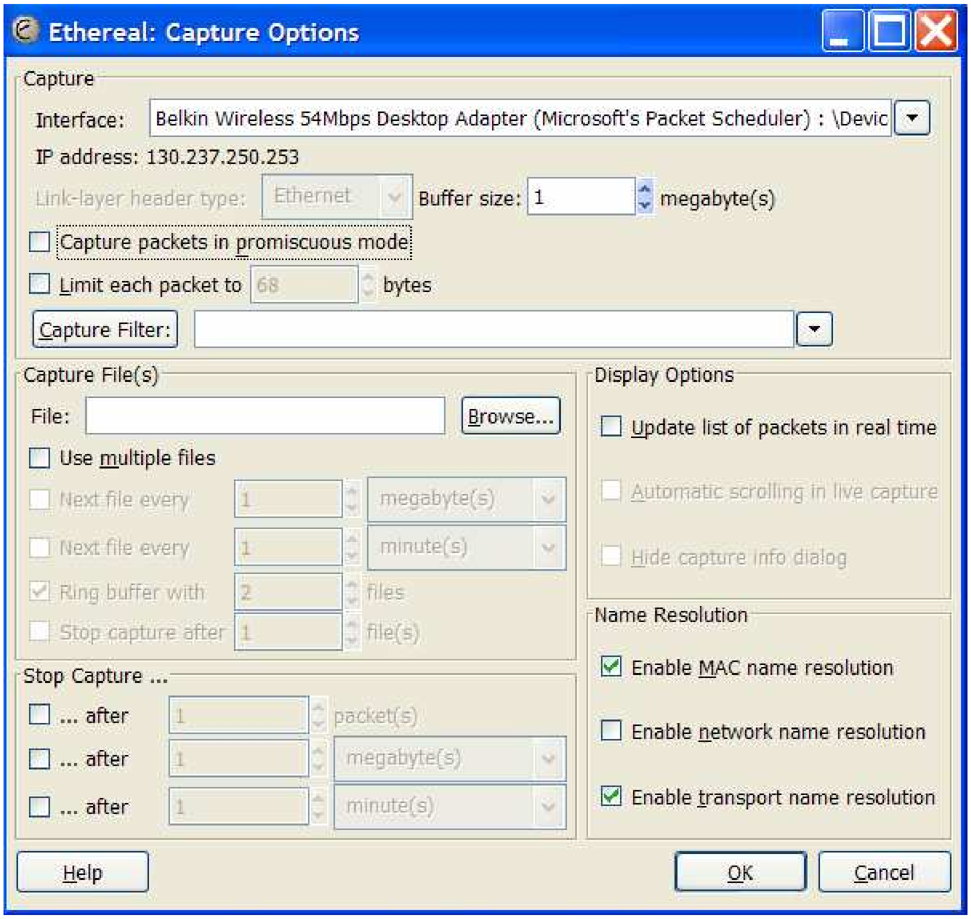
Assuming that you are running Red Hat Linux or Windows, you should install Ethereal (a packet analyzer). It is available on the website:
http://www.ethereal.com
More specifically
http://www.ethereal.com/download.html

Laboration

1. Start Ethereal. The following window will appear on the on the screen.


The Ethereal Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Ready to load or capture
No Packets

2. The top pane of this window is the **packet list pane** will give a list of packets captured. Any packet selected in this pane will be shown in detail in the other two panes. The middle pane is the **tree view pane**. This shows the contents of packets in a hierarchical (i.e. tree-like) way. The bottom pane is the **data view pane**. This gives a hexadecimal dump of the contents of a packet.
3. You can start up ethereal by clicking on **capture>start** on top of the ethereal window. This will cause the following sub window to appear. Click on OK.



Ethereal: Capture Options

Capture

Interface: Belkin Wireless 54Mbps Desktop Adapter (Microsoft's Packet Scheduler) : \Devic

IP address: 130.237.250.253

Link-layer header type: Ethernet Buffer size: 1 megabyte(s)

□ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File:

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

□ Update list of packets in real time

□ Automatic scrolling in live capture

□ Hide capture info dialog

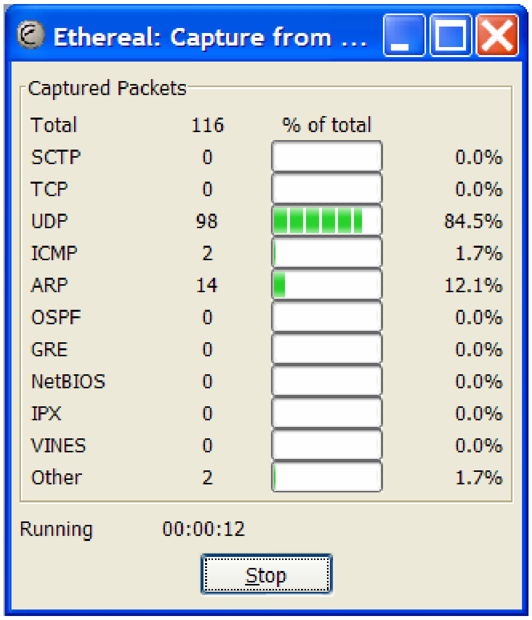
Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

4. Ethereal will now start capturing packets. The following window will show a record of packets captured.



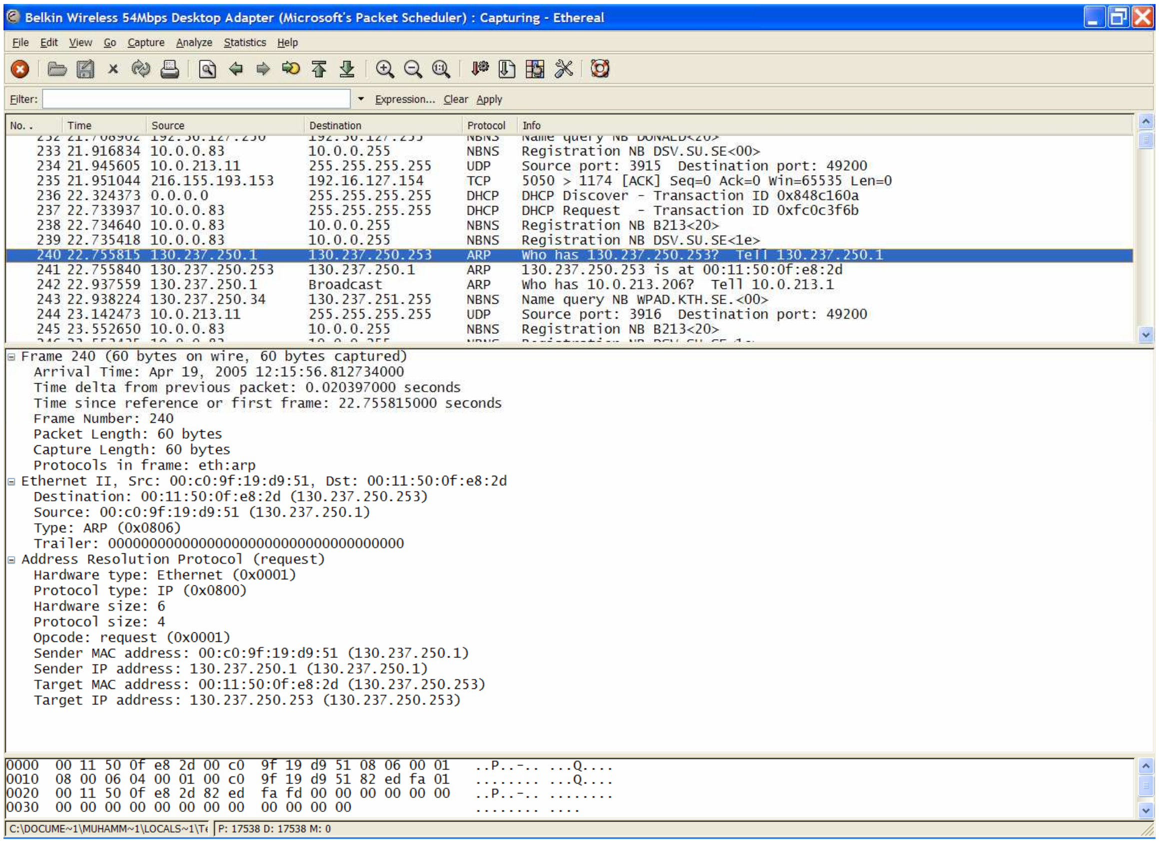
Ethereal: Capture from ...

Captured Packets

Total	116	% of total
SCTP	0	0.0%
TCP	0	0.0%
UDP	98	84.5%
ICMP	2	1.7%
ARP	14	12.1%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	2	1.7%

Running 00:00:12

5. Try to capture ARP request and reply packets as shown.


Belkin Wireless 54Mbps Desktop Adapter (Microsoft's Packet Scheduler) : Capturing - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time      Source           Destination      Protocol Info
233 21.916834 10.0.0.83        10.0.0.255       NBNS  Registration NB DSV.SU.SE<00>
234 21.945605 10.0.213.11      255.255.255.255  UDP   Source port: 3915  Destination port: 49200
235 21.951044 216.155.193.153  192.16.127.154   TCP   5050 > 1174 [ACK] Seq=0 Ack=0 Win=65535 Len=0
236 22.324373 0.0.0.0          255.255.255.255  DHCP  DHCP Discover - Transaction ID 0x848c160a
237 22.733937 10.0.0.83        255.255.255.255  DHCP  DHCP Request  - Transaction ID 0xfc0c3f6b
238 22.734640 10.0.0.83        10.0.0.255       NBNS  Registration NB B213<20>
239 22.735418 10.0.0.83        10.0.0.255       NBNS  Registration NB DSV.SU.SE<1e>
240 22.755815 130.237.250.1    130.237.250.253  ARP   Who has 130.237.250.253?  Tell 130.237.250.1
241 22.755840 130.237.250.253  130.237.250.1    ARP   130.237.250.253 is at 00:11:50:0f:e8:2d
242 22.937559 130.237.250.1    Broadcast        ARP   Who has 10.0.213.206?  Tell 10.0.213.1
243 22.938224 130.237.250.34   130.237.251.255  NBNS  Name query NB WPAD.KTH.SE.<00>
244 23.142473 10.0.213.11      255.255.255.255  UDP   Source port: 3916  Destination port: 49200
245 23.552650 10.0.0.83        10.0.0.255       NBNS  Registration NB B213<20>
```

```
⊟ Frame 240 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Apr 19, 2005 12:15:56.812734000
    Time delta from previous packet: 0.020397000 seconds
    Time since reference or first frame: 22.755815000 seconds
    Frame Number: 240
    Packet Length: 60 bytes
    Capture Length: 60 bytes
    Protocols in frame: eth:arp
⊟ Ethernet II, Src: 00:c0:9f:19:d9:51, Dst: 00:11:50:0f:e8:2d
    Destination: 00:11:50:0f:e8:2d (130.237.250.253)
    Source: 00:c0:9f:19:d9:51 (130.237.250.1)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:c0:9f:19:d9:51 (130.237.250.1)
    Sender IP address: 130.237.250.1 (130.237.250.1)
    Target MAC address: 00:11:50:0f:e8:2d (130.237.250.253)
    Target IP address: 130.237.250.253 (130.237.250.253)
```

```
0000  00 11 50 0f e8 2d 00 c0  9f 19 d9 51 08 06 00 01   ..P..-.. ...Q....
0010  08 00 06 04 00 01 00 c0  9f 19 d9 51 82 ed fa 01   ........ ...Q....
0020  00 11 50 0f e8 2d 82 ed  fa fd 00 00 00 00 00 00   ..P..-.. ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

C:\DOCUME~1\MUHAMM~1\LOCALS~1\Te P: 17538 D: 17538 M: 0

6. Enter the contents of the request and reply in the following format for ARP header.

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation
Request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address</td></tr>
<tr><td colspan="3">Sender protocol address</td></tr>
<tr><td colspan="3">Target hardware address</td></tr>
<tr><td colspan="3">Target protocol address</td></tr>
</table>

7. Now highlight a UDP packet and fill in the following IP and UDP header.

IP Header

<table>
<tr><td>VER
4 bits</td><td>HLEN
4bits</td><td>DS
8 bits</td><td colspan="2">Total length
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time to live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Option</td></tr>
</table>

UDP Header

Source port number 16 bits	Destination port number 16 bits
Total length 16 bits	Checksum 16 bits

8. Now find DHCP messages (DISCOVER, OFFER, REQUEST and ACK) to offer an IP address.
9. Which ports have been used by DHCP?
10. Fill in the DHCP header for all the four DHCP messages. Try to observe the differences among them.

<table>
<tr><td>Operation code</td><td>Hardware type</td><td colspan="2">Hardware length</td><td>Hop count</td></tr>
<tr><td colspan="5">Transaction ID</td></tr>
<tr><td colspan="2">Number of seconds</td><td>F</td><td colspan="2">Unused</td></tr>
<tr><td colspan="5">Client IP address</td></tr>
<tr><td colspan="5">Your IP address</td></tr>
<tr><td colspan="5">Server IP address</td></tr>
<tr><td colspan="5">Gateway IP address</td></tr>
<tr><td colspan="5">Client hardware address</td></tr>
<tr><td colspan="5">Server name</td></tr>
<tr><td colspan="5">Boot file name</td></tr>
<tr><td colspan="5">Options</td></tr>
</table>

11. Stop ethereal and start capturing the packets again for the next steps.
12. Lets ping YAHOO, using the command:

    ping www.yahoo.com

13. Record the ICMP header for request and reply.

Type	Code	Checksum
Identifier		Sequence number
Optional data		

14. What type of changes you note in ICMP packets?
15. Now lets find the hops to YAHOO. Use the command:

    traceroute www.yahoo.com (Linux)
    tracert www.yahoo.com (Windows)

16. Capture the ICMP packets and note the changes.
17. Now we will try to send one packet to YAHOO.

    ping –c 1 –s 2000 www.yahoo.com (Linux)
    ping –n 1 –l 2000 www.yahoo.com (Windows)

18. Do you expect fragmentation? If so, capture the IP fragments and record the IP headers to see the differences in fragments.
19. Now try to get more fragments.

    ping –c 1 –s 4000 www.yahoo.com (Linux)
    ping –n 1 –l 4000 www.yahoo.com (Windows)

20. Again capture the fragments and note IP header fields.
21. Start capture and go to YAHOO.
22. Select DNS query and response packets and record the fields in following format:

DNS Header

Identification	Flags
Number of question records	Number of answer records
Number of authoritative records	Number of additional records

Question Record

Query name	
Query type	Query class

Resource Record

<table>
<tr><td colspan="2">Domain name</td></tr>
<tr><td>Domain type</td><td>Domain class</td></tr>
<tr><td colspan="2">Time to live</td></tr>
<tr><td>Resource data length</td><td>Resource data</td></tr>
<tr><td colspan="2">Resource data</td></tr>
</table>

23. Try to find out all the name servers involved in resolving www.yahoo.com.
24. Now browse www.it.kth.se, capture the packets and look for the keep alives that the network send to tell that you are still there (if you are not, you have to relogin to have network connectivity). How often do these packets come? How they look like?