Lab 1: Packet Capture (Network Interface)

Details

Aim: To provide a foundation in reading data packets

Activities

If Visual Studio is installed on your machine, download the following solution [1]:

http://www.dcs.napier.ac.uk/~bill/WinPCap1.zip

It has the following code [1]:

```
using System;
using Tamir.IPLib;

namespace NapierCapture
{

   public class ShowDevices
   {

      public static void Main(string[] args)
      {
         string verWinPCap =null;
         int count=0;

         verWinPCap= Tamir.IPLib.Version.GetVersionString();

         PcapDeviceList getNetConnections = SharpPcap.GetAllDevices();

         Console.WriteLine("WinPCap Version: {0}", verWinPCap);

         Console.WriteLine("Connected devices:\r\n");

         foreach(PcapDevice net in getNetConnections)
         {
            Console.WriteLine("{0}) {1}",count,net.PcapDescription);
            Console.WriteLine("\tName:\t{0}",net.PcapName);
            Console.WriteLine("\tMode:\t\t\t{0}",net.PcapMode);
            Console.WriteLine("\tIP Address: \t\t{0}",net.PcapIpAddress);
            Console.WriteLine("\tLoopback: \t\t{0}",net.PcapLoopback);

            Console.WriteLine();
            count++;
         }

         Console.Write("Press any <RETURN> to exit");
         Console.Read();

      }
   }
}
```

Run the program, and verify that it produces a list of the available network cards, such as:

```
WinPCap Version: 1.0.2.0
Connected devices:
```

```
0) Realtek RTL8169/8110 Family Gigabit Ethernet NIC
    (Microsoft's Packet Scheduler)
        Name:   \Device\NPF_{A22E93C1-A78D-4AFE-AD2B-517889CE42D7}
        Mode:                   Capture
        IP Address:             192.168.2.1
        Loopback:               False

1) Intel(R) PRO/Wireless 2200BG Network Connection (Microsoft's Packet Scheduler)
        Name:   \Device\NPF_{044B069D-B90A-4597-B99E-A68C422D5FE3}
        Mode:                   Capture
        IP Address:             192.168.1.101
        Loopback:               False
```

List the network cards in your machine:

Next update the code so that it displays the information on the network connections [1]:

```
foreach(PcapDevice net in getNetConnections)
{
  Console.WriteLine("{0}) {1}",count,net.PcapDescription);

  NetworkDevice netConn = (NetworkDevice)net;

  Console.WriteLine("\tIP Address:\t\t{0}",netConn.IpAddress);
  Console.WriteLine("\tSubnet Mask:\t\t{0}",netConn.SubnetMask);
  Console.WriteLine("\tMAC Address:\t\t{0}",netConn.MacAddress);
  Console.WriteLine("\tDefault Gateway:\t{0}",netConn.DefaultGateway);
  Console.WriteLine("\tPrimary WINS:\t\t{0}",netConn.WinsServerPrimary);
  Console.WriteLine("\tSecondary WINS:\t\t{0}",netConn.WinsServerSecondary);
  Console.WriteLine("\tDHCP Enabled:\t\t{0}",netConn.DhcpEnabled);
  Console.WriteLine("\tDHCP Server:\t\t{0}",netConn.DhcpServer);
  Console.WriteLine("\tDHCP Lease Obtained:\t{0}",netConn.DhcpLeaseObtained);
  Console.WriteLine("\tDHCP Lease Expires:\t{0}",netConn.DhcpLeaseExpires);
  Console.WriteLine();
  count++;
}
```

A sample run shows the details of the network connections [1]:

```
1) Intel(R) PRO/Wireless 2200BG Network Connection (Microsoft's Packet Scheduler)
        IP Address:             192.168.1.101
        Subnet Mask:            255.255.255.0
        MAC Address:            0015003402F0
        Default Gateway:        192.168.1.1
        Primary WINS:           0.0.0.0
        Secondary WINS:         0.0.0.0
        DHCP Enabled:           True
        DHCP Server:            192.168.1.1
        DHCP Lease Obtained:    03/01/2006 10:44:40
        DHCP Lease Expires:     04/01/2006 10:44:40
```

List the details of the connections on your PC:

[1] This code is based on the code wrapper for WinPCap developed by T.Gal [http://www.thecodeproject.com/csharp/sharppcap.asp].