Instituto Politécnico Nacional

Escuela Superior de Cómputo

Unidad de Aprendizaje

Redes de Computadoras

Alumno

Alejandro Hernandez Gomez

Profesor

Moreno Cervantes Axel Ernesto

Practica 2 Instalación y Uso de la Biblioteca Jnetpcap

Introducción

En esta práctica aprenderemos cual es la instalación y cuáles son los componentes necesarios para utilizar la librería jNetPcap. Para la practica utilizaremos en IDE NetBeans y sus componentes además de que se mostrara un ejemplo del uso de esta librería capturando tramas y mostrando su direcciones de MAC destino y origen, el tipo y en base al tipo su protocolo.

Esta es una librería de código abierto que ayuda a capturar paquetes en tiempo real y decodificarlos.

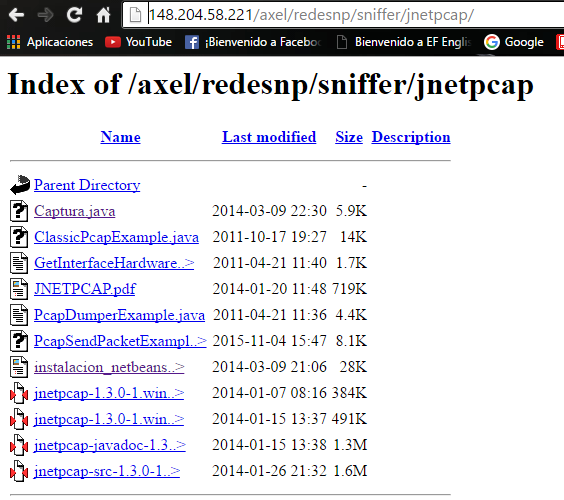
También tiene una extensa librería de protocolos de redes.

El ejemplo que se utilizara en esta práctica es un analizador de protocolos mejor conocido como SNIFFER.

El SNIFFER en un programa que captura las tramas de una red de computadoras para su análisis.

Desarrollo

Entrar a la liga http://148.204.58.221/axel/redesnp/sniffer/jnetpcap



Y descargar los archivos

jnetpcap-1.3.0-1.win64

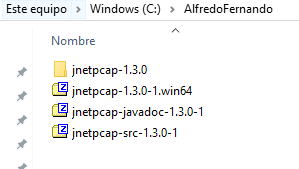
jnetpcap-javadoc-1.3.0-1

jnetpcap-src-1.3.0-1

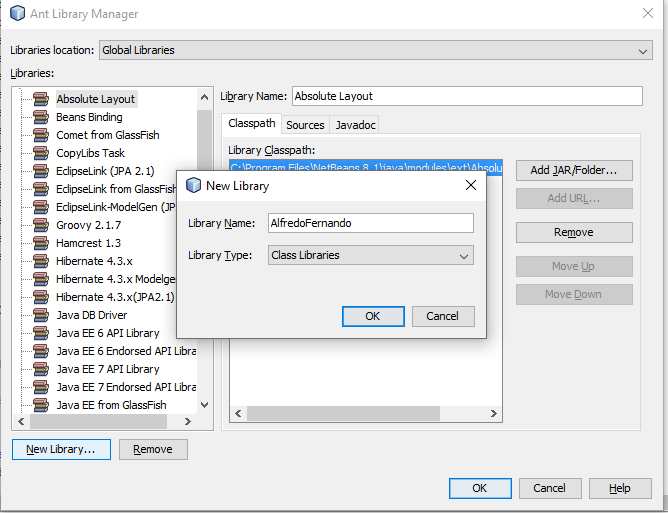
Captura.java

Instalacion\_netbeans.pdf

Leer por completo el documento “Intalacion\_netbeans.pdf” y crear una biblioteca (asignarle el nombre de ustedes) que contenga los paquetes de jnetcap.



En el menú TOOLS seleccionar libraries y luego New Library



Hacer click en la opción “Classpath” luego hacer click en el botón "Add JAR/Folder..." y seleccionar el archivo “jnetpcap.jar”.

Ir a la opción Sources, luego hacer click en el botón "Add JAR/Folder..." y seleccionar el archivo “jnetpcap-src-1.3.0-1”

Ir a la opción Javadoc, luego hacer click en el botón "Add JAR/Folder..." y seleccionar el archivo “jnetpcap-javadoc-1.3.0-1”

Luego seleccionamos el botón de OK

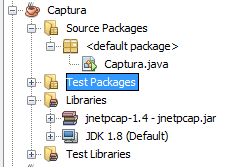
Seleccionamos del menú "Run->Setup Project Configuration->Customize..." y aparecerá una ventana. Luego seleccionar el botón “New” que se encuentra al lado derecho de “Configuration” y le hacemos click en Ok.

Finalmente en el cuadro de texto de “VM Options” pegamos lo siguiente

-Djava.library.path="C:\libs \jnetpcap-1.3.0"

Y presionamos OK

Crear un nuevo proyecto y copiar el archivo “Captura.java”



Modificar el código para que captura 20 tramas e imprima de cada una de ellas la Dirección MAC Origen y Destino, el tipo y en base al tipo el protocolo.

Codigo agregado

System.out.printf("\nMAC Destino: ");

for(int i=0; i<6; i++){

if(i==5){

System.out.printf("%02X",packet.getUByte(i));

}

else

System.out.printf("%02X-",packet.getUByte(i));

}

System.out.printf("\nMAC Origen: ");

for(int i=6; i<12; i++){

if(i==11){

System.out.printf("%02X",packet.getUByte(i));

}

else

System.out.printf("%02X-",packet.getUByte(i));

}

System.out.printf("\nTipo: %02X:%02X\n",packet.getUByte(12),packet.getUByte(13));

String a = Byte.toString(packet.getByte(12))+Byte.toString(packet.getByte(13));

if(a.equals("00") || a.equals("5DC"))

System.out.println("Protocolo: IEEE802.3 Length Field");

if(a.equals("101") || a.equals("1FF"))

System.out.println("Protocolo: Experimental");

if(a.equals("20"))

System.out.println("Protocolo: Experimental");

if(a.equals("21"))

System.out.println("Protocolo:PUP Addr Trans (see 0A01)");

if(a.equals("60"))

System.out.println("Protocolo: XEROX NS IDP");

if(a.equals("80"))

System.out.println("Protocolo: DOD IP");

if(a.equals("81"))

System.out.println("Protocolo: X.75 Internet");

if(a.equals("82"))

System.out.println("Protocolo: NBS Internet");

if(a.equals("83"))

System.out.println("Protocolo: ECMA Internet");

if(a.equals("84"))

System.out.println("Protocolo: Chaosnet");

if(a.equals("0805"))

System.out.println("Protocolo: X.25 Level 3");

if(a.equals("86"))

System.out.println("Protocolo: ARP");

if(a.equals("87"))

System.out.println("Protocolo: XNS Compatability");

if(a.equals("81C"))

System.out.println("Protocolo: Symbolics Private ");

if(a.equals("888") || a.equals("088A"))

System.out.println("Protocolo: Xyplex ");

if(a.equals("90"))

System.out.println("Protocolo:Ungermann-Bass net debugr");

if(a.equals("A0"))

System.out.println("Protocolo: Xerox IEEE802.3 PUP");

if(a.equals("A1"))

System.out.println("Protocolo: PUP Addr Trans");

if(a.equals("BAD "))

System.out.println("Protocolo: Banyan Systems");

if(a.equals("100"))

System.out.println("Protocolo: Berkeley Trailer nego");

if(a.equals("160"))

System.out.println("Protocolo: Valid Systems ");

if(a.equals("4242"))

System.out.println("Protocolo: PCS Basic Block Protocol");

if(a.equals("528"))

System.out.println("Protocolo: BBN Simnet");

if(a.equals("600"))

System.out.println("Protocolo: DEC Unassigned (Exp.)");

if(a.equals("601"))

System.out.println("Protocolo: DEC MOP Dump/Load ");

if(a.equals("602"))

System.out.println("Protocolo:DEC MOP Remote Console");

if(a.equals("603"))

System.out.println("Protocolo:DECDECNETPhaseIV oute");

if(a.equals("604"))

System.out.println("Protocolo: DEC LAT ");

if(a.equals("605"))

System.out.println("Protocolo: DEC Diagnostic Protocol");

System.out.printf("\nNumero de trama: %d\n", x++);

Conclusión

Alejandro Hernandez Gomez

En esta práctica aprendimos el uso básico de la librería jNetpCap aplicando un ejemplo ya hecho y modificando este para que muestre algunos de los componentes más importantes de las tramas.

En general la práctica no estuvo muy difícil, pero si un poco confusa respecto a cómo el programa hacia la captura de los paquetes, pues para poder realizar la práctica, primero teníamos que analizar el código y que es lo que hace cada sección.

Otra de las complicaciones para algunos fue a la hora de agregar una librería pues muchos no estamos acostumbrados a usar IDEs como ese.