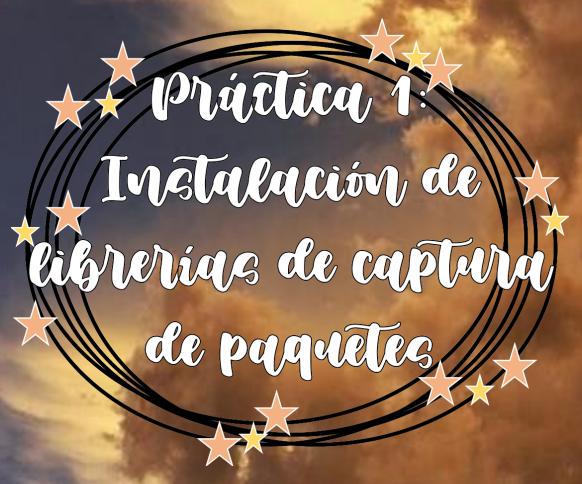




# INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO

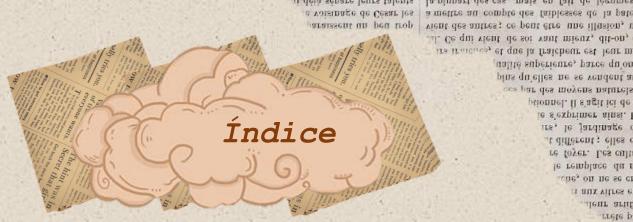


**INTEGRANTES:** 

GONZÁLEZ MORA ERIKA GISELLE OLIVARES MÉNEZ GLORIA OLIVA

**PROFESOR: Moreno Cervantes Axel Ernesto** 

REDES DE COMPUTADORAS 2CV16 11/03/2021



1.	Introducción	3
	Desarrollo	
	Conclusiones	
	Bibliografía	
	Anexos	
٦.	1 IIICAOS	

ualité superieure, parce qu'on pins qu'elles ne se vendent a ces par des moyens naturels le s'exprimer ainsi. I ptionnel. Il s'agit ici de

irs, le jardinage at différent ; elles e re foyer. Les cult

le remplace du r .che, on ne se cr n aux vitres e

deur artif rrete p

wind same and a Manage que les personnages accessoires concourenta rehausser re accrue par un artifice inan dejà separe feurs talents e vousinage de César les araissent un peu trop

à la halle, il y introduira des espèces r renore-rans dorvent être sacrifies; il faut pas seulement les legumes qu'on trouv is les artistes? Dans toute com- teur de bonnes choses doit avoir son pot verite dans toute la rigueur du mot. Un la plupart des cas, mais en fait de leg a mettre au compte des faiblesses de la vient des autres; ce peut être une illus al. Ce qui vient de soi vant mieux, di ars traicaes, et que la fraicheur est le

men'st less month and

ptionnel. Il s'agit i e s'exprimer a irs, le jardin t différent ; e re foyer. Le le remplace one, on ne TIGHL

ualité superieure, parce

pins qu'elles ne se vend ce par des moyens na

#### 1. Introducción

#### 1.1. Instalación de librerías de captura de paquetes

Para realizar aplicaciones escritas en lenguaje C que necesiten realizar captura de paquetes o tramas ethernet, es necesaria la instalación de una librería esencial. En la práctica se hará uso del paquete de librerías de npcap.

portent

Aclaremos que, durante 14 años, WinPcap fue el paquete libpcap estándar para Windows. Pero cuando este lanzó Windows 10 sin compatibilidad con NDIS 5, WinPcap no pudo mantenerse al día.

Windows 10 introdujo requisitos estrictos de firma de controladores que WinPcap no puede cumplir. Y npcap es totalmente compatible, con sus controladores probados y confirmados por Microsoft.

Construido sobre la base de código WinPcap probada y verdadera, con una serie de nuevas características interesantes y ampliamente probado con las versiones actualmente compatibles de Windows, Npcap es el futuro de WinPcap.

También, para realizar aplicaciones escritas en lenguaje Java que necesiten realizar captura de paquetes o tramas ethernet, es necesaria la instalación de esta librería importante. Además de realizar la configuración de la biblioteca PCAP4J en NetBeans. Aquí es esencial el registro de nuevas variables de entorno dado que npcap será instalado en Windows\System32\Npcap\ por default. En la siguiente práctica se mostrarán los pasos que se siguen para la realización de estas actividades en c y java.

#### 2. Desarrollo

#### 2.2. Encapsulación del paquete

La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU de Capa 3 para encapsular el mensaje que se envía.

Tanto el encabezado como el tráiler de Ethernet tienen varias secciones de información que el protocolo Ethernet utiliza. Cada sección de la trama se denomina campo. Hay dos estilos de tramas de Ethernet: el IEEE 802.3 (original) y el IEEE 802.3 revisado (Ethernet).

Las diferencias entre los estilos de tramas son mínimas. La diferencia más significativa entre el IEEE 802.3 (original) y el IEEE 802.3 revisado es el agregado de un delimitador de inicio de trama (SFD) y un pequeño cambio en el campo Tipo que incluye la Longitud, tal como se muestra en la siguiente figura.

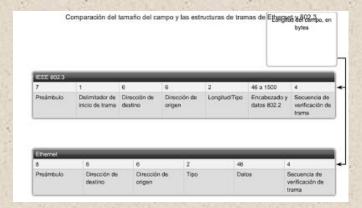


Fig. 1. IEEE 802.3 original vs IEEE 802.3 revisado.

#### 2.3. Tamaño de la trama de Ethernet

at different; elles consti El estándar Ethernet original definió el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes. Esto incluve todos los bytes del compo Direcció del compo Direcci Secuencia de verificación de trama (FCS). Los campos Preámbulo y Delimitador de inicio de trama no se incluyen en la descripción del tamaño de una trama. El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes. Se aumentó el tamaño de la trama para que se adapte a una tecnología denominada Red de área local virtual (VLAN). Las VLAN se crean dentro de una red presentarán Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas y, por lo tanto, se consideran no válidas.

Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (1 byte) se utilizan para la sincronización entre los dispositivos de envío y de recepción. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.

# 2.4. Campo Dirección MAC de destino

El campo Dirección MAC de destino (6 bytes) es el identificador del receptor deseado. Como recordará, la Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

# 2.5. Campo Dirección MAC de origen

El campo Dirección MAC de origen (6 bytes) identifica la NIC o interfaz que origina la trama. Los switches también utilizan esta dirección para ampliar sus tablas de búsqueda. El rol de los switches se analizará más adelante en este capítulo.

#### 2.6. Campo Longitud/Tipo

El campo Longitud/Tipo (2 bytes) define la longitud exacta del campo Datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. En este campo debe ingresarse una longitud o un tipo. Sin embargo, sólo uno u otro podrá utilizarse en una determinada implementación. Si el objetivo del campo es designar un tipo, el campo Tipo describe qué protocolo se implementa.

El campo denominado Longitud/Tipo sólo aparecía como Longitud en las versiones anteriores del IEEE y sólo como Tipo en la versión DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que ambos usos eran comunes. El campo Tipo de la Ethernet II se incorporó a la actual definición de trama del 802.3. La Ethernet II es el formato de trama de Ethernet que se utiliza en redes TCP/IP. Cuando un nodo recibe una trama, debe analizar el campo Longitud/Tipo para determinar qué protocolo de capa superior está presente. Si el valor de los dos octetos es equivalente a 0x0600 hexadecimal o 1536 decimal o mayor que éstos, los contenidos del campo Datos se codifican según el protocolo indicado.

#### 2.7. Campos Datos y Relleno

Los campos Datos y Relleno (de 46 a 1500 bytes) contienen los datos encapsulados de una capa superior, que es una PDU de Capa 3 genérica o, con mayor frecuencia, un paquete IPv4. Todas las tramas deben

irs, le jardinage de tou

le remplace du mier che, on ne se croi et aux vitres et a deur artific

rrete pa

to les personnages, accome de accidentation un peu trong les personnages, accome de accession de la trong de la constant de la

tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, el Pad se utiliza para aumentar el tamaño de la trama hasta alcanzar este tamaño mínimo.

#### 2.8. Campo Secuencia de verificación de trama

El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama.

El dispositivo receptor recibe la trama y genera una CRC para detectar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama. Un cambio en los datos podría ser resultado de una interrupción de las señales eléctricas que representan los bits.



Fig. 2. Secuencia de verificación de trama Ethernet.

### 2.9. Compilación de ejemplos NPCAP en c

Lo primero que tenemos que hacer es instalar Npcap en Windows. Lo descargamos de la página oficial, ejecutamos el archivo .exe y nos aparecerá una ventana para aceptar los Términos y Condiciones.

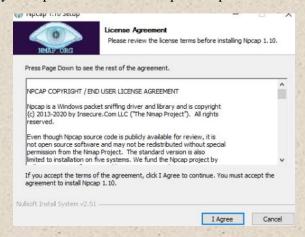


Fig. 3. Términos y Condiciones Npcap.

Aceptamos y en la siguiente ventana (opciones de instalación) habilitamos la opción de compatibilidad con WinPcap.

the hint was

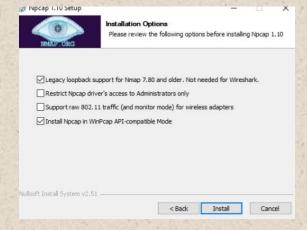


Fig. 4. Opciones de Instalación.

Posteriormente, comenzamos el proceso de instalación al presionar el botón "Install".

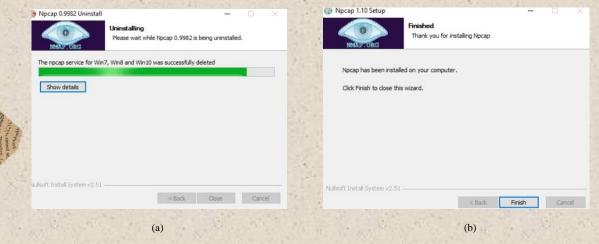


Fig. 5. Instalación. (a) Inicio, (b) Finalización.

Lo siguiente que debemos hacer es descargar los archivos .zip que se encontrarán en la pantalla mostrada a continuación (npcap-1.10. zip y npcap-sdk-1.06.zip).

#### Index of /axel/redesnp/sniffer/NPCAP Last modified Size Description Parent Directory Compilación de ejemp.. > 2021-03-07 18:42 130K captura.c 2021-03-08 09:07 3.0K envia.c 2021-03-07 18:38 2.9K npcap-1.10.exe 2021-01-12 18:21 773K npcap-1.10.zip 2021-01-12 18:21 722K npcap-sdk-1.06.zip 2021-01-12 18:21 333K

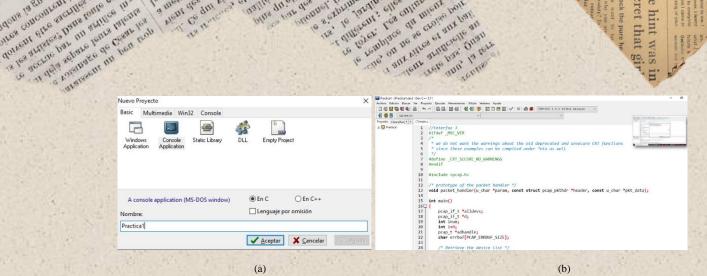
Fig. 6. Página donde se encuentran los archivos.

Extraemos los archivos de ambas carpetas en direcciones donde podamos acceder fácilmente a ellas. Ahora, abrimos el entorno de desarrollo Dev-C++ y generamos un proyecto, en este caso aplicación desde consola en el lenguaje C, y adicionamos el archivo captura.c (véase el programa en anexos) colocado en la pantalla de la Fig. 6.

t different; elles consti re foyer. Les cultures

le remplace du mier che, on ne se crois

or aux vitres et a deur arude rrete pa



Lemby GCG

cresines concounter Se dorvent erre sacriff

Fig. 7. Proyecto. (a) Generación, (b) Colocación de archivo.

A continuación, abrimos las opciones del proyecto y nos vamos a la pestaña de Compilador, se debe verificar que tenga el que se muestra en la siguiente pantalla.

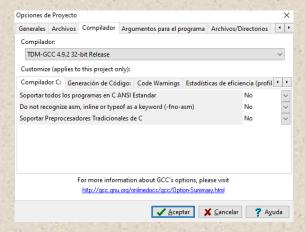


Fig. 8. Opciones de Proyecto - Compilador.

Ahora, tenemos que agregar los parámetros. Así que nos movemos a la pestaña de Argumentos para el programa y enlazar la biblioteca wpcap.lib ubicada en la ruta (npcap/Lib/wpcap.lib).

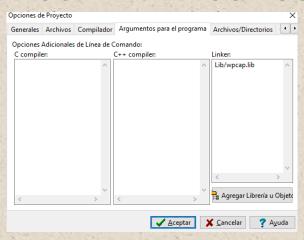


Fig. 9. Opciones de Proyecto – Argumentos para el Programa.

Luego establecemos los directorios de bibliotecas en la pestaña Archivos/Directorios, subpestaña Directorios de Librerías (.a .lib .dll) como se muestra en la Fig. 10.

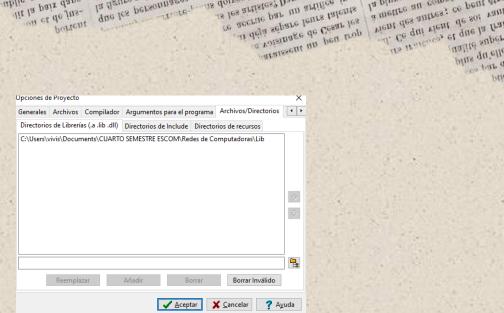


Fig. 10. Directorios de Bibliotecas.

También establecemos los directorios de los archivos include en la subpestaña Directorios de Include.

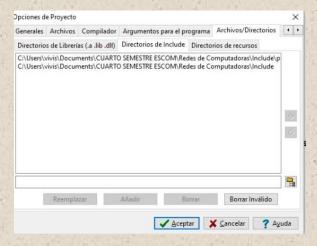


Fig. 11. Directorios de Include.

#### Seleccionamos la opción de Aceptar.

ablic

lit la paix dans

on et de jus-

portent

la Benro

que les personnage

-Plicte-

is les artistes? De

ce accrue par un aminas :

d. Ce qui vient de soi vaut miamini urs trateues, et que la fraicheur est leur mer

plus qu'elles ne se vendent au par des moyens naturels ptionnel. Il s'agit ici de le s'exprimer ainsi. 118, le jardinage a different; elle

re foyer. Les c

le remplace

che, on ne

aux vi

Ya de regreso en la hoja de trabajo, en la barra superior, podemos apreciar diversos íconos. Daremos al ícono con pequeños cuadros grises, es la opción de reconstruir todo. Después de seleccionar dicho ícono se iniciará el proceso de compilación con las nuevas modificaciones que hicimos en las opciones del proyecto.

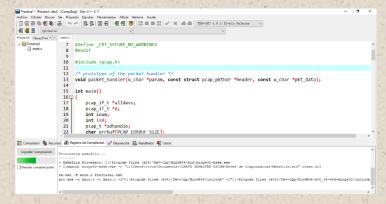


Fig. 12. Compilación.

# Funcionamiento del programa

ublic so dit la paix dans

on et de jus- la flanne met

portent que les personnages

re foyer. Les culture Luego de compilar el programa, si todo salió sin contratiempos nos mostrará una pantalla como la siguiente: le temblace du mit

-Profe-y-als dorvers

As les artistes? Dane ve accrue par un artifice in

.ii dėja sėpare leurs talents | Ja nimari

e voisinage de Gesar les à mettre au rounes

araissent un peu trop vient des autres; ce nom sam

ed. Ce qui vient de soi vaut mieux du

118 If alcaes, et que la fraicheur est leur ménio

pins qu'elles ne se vendent au mare oes par des moyens naturels et fac ptionnel. Il s'agit ici de plante le s'exprimer ainsi. Le foi

urs, le jardinage de to at different; elles cons

che, on ne se cro a aux vitres et deur artiff rrete p

```
Compilation results...
Errors: 0
 wallings: O

Output Filename: C:\Users\vivis\Documents\CUARTO SEMESTRE ESCOM\Redes de Computadoras\Practical.exe

Output Size: 104.4638671875 KIB

Compilation Time: 16.56s
```

Fig. 13. Resultados de Compilación Exitosa.

Ahora, regresamos a los pequeños íconos de la parte superior, pero ahora seleccionaremos el que tiene 4 cuadros de colores pequeños y sin separación entre sí. El ícono se llama Compilar y Ejecutar. Esto es, como dice su nombre, para que ejecutemos el programa y veamos el resultado del código.

Posteriormente nos aparecerá la consola de Windows con el resultado del programa:

```
(MdisWan Adapter)
(MdisWan Adapter)
(MdisWan Adapter)
(Microsoft)
(Omacle)
(Microsoft)
(MdicWan Adapter)
capture)
(Realtek PCIe FE Family Controller)
```

Fig. 14. CMD Windows.

Nos despliega la lista de las tarjetas de red instaladas en nuestro equipo, y se nos preguntará el número de la tarjeta que deseamos usar para realizar el envío de las tramas (véase la figura 14).

Una vez que digitamos el número de la tarjeta de red, el cual en este caso fue el 4 (véase la figura 15 a), que queremos usar se nos desplegará una lista de 15 tramas enviadas y se nos mostrará la trama, la dirección MAC de destino, la dirección MAC de origen, y el campo tipo con su equivalente en número decimal. Con este paso termina la ejecución de nuestro programa (véase la figura 15 b y 15 c).

```
lgen:
44: D5: 05: F7:
 2048 08 00
destino:
2:44:D5:05:F7:
origen:
16: 32: C1: 6E: 86:
     igen:
32: C1: 6E: 86:
                                                                                                                       (b)
```

lit la pair on et de jus-

portent que les paren-

-Pluche-

As les arties

ce accrue par un sacia

ai deja separe leurs talente

e voisinage de Gesar les a maine

araissent un peu trop vient des anteses

d. Ce qui vient de soi vant

118 Wateres, et que la fraicheur est 1

nalité superieure, parce qu'on les a t plus qu'elles ne se vendent au mare es par des moyens naturels et (20 ptionnel. Il s'agit ici de plant

e s'exprimer ains. Le fo irs, le jardinage de t A different; elles cons re foyer. Les culture le remplace du mi che, on ne se cro it aux vitres et deur artit

-rrete !

```
C:\Users\vivis\Documents\CUARTO SEMESTRE ESCOM\Redes de Computadoras\Practica1.ex
      : 2048 08 00
destino:
2:44:D5:05:F7:
     origen:
16: 32: C1: 6E: 86:
    po: 2048 08 00
     ess exited after 8.744 seconds with return value 0 ione una tecla para continuar . . .
```

(c) Fig. 15. Capturas. (a) Parte 1, (b) Parte 2, (c) Parte 3.

# Solistingen un peu trop Went Se qui 2.10. Configuración de biblioteca PCAP4J en NetBeans

118, 16

A different; elle

re forer remplace.

1. Instalación de NPCAP en Windows:

A. Ce dill Gas el

Dalle Mis direct . C. 1.9L 968 Monnel ie sexurine

Dado que npcap será instalado en Windows\System32\Npcap\ por default, necesitas hacer lo siguiente para que NPCAP pueda ser cargado (véase la figura 21):

Agrega la variable de entorno jna.library.path a Windows \System32\Npcap\.

The th He so Choise Whit

Weite artificial dis

entorno org.pcap4j.core.pcapLibName Agrega la variable de Windows \System32\Npcap\wpcap.dll org.pcap4j.core.packetLibName Windows \System32\Npcap\Packet.dll.

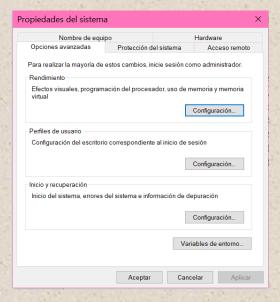


Fig. 16. Propiedades del sistema donde se agregan variables de entorno.

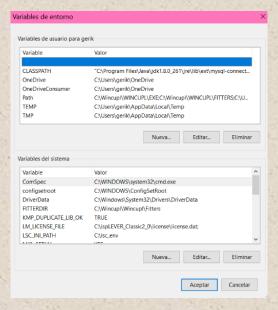


Fig. 17. Variables de entorno.

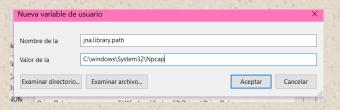


Fig. 18. Adición de la primer variable de entorno jna.library.path.

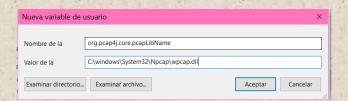


Fig. 19. Adición de la segunda variable de entorno org.pcap4j.core.pcapLibName.

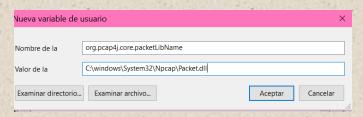


Fig. 20. Adición de la tercera variable de entorno org.pcap4j.core.packetLibName.

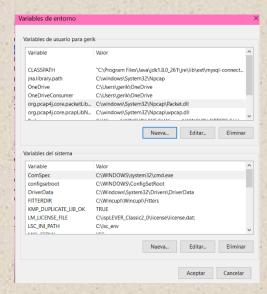


Fig. 21. Todas las variables de entorno ya agregadas.

ptionnel. Il s'agit ici de p'at le s'exprimer ainsi, Le us, le jardinage de at different; elles co

re foyer. Les cultu le remplace du n

che, on ne se c aux vitres

denr ar

d. Ce qui vi 63 FAF des le sexuitation diffren; elles To difer, Les culture in the contract of the then The off He se cidisc White A SHE WATER PLANT THE Will William being Leady Was ida-Atheres to the tree top

Monnel.

steen lans tome dela sipare legis dacing par un artilice in

d men vient des malle Mis dir. bir

2. Instala npcap en modo con compatibilidad con WinPcap (habilitar la compatibilidad durante el proceso de instalación) se puede observar en la figura 22.

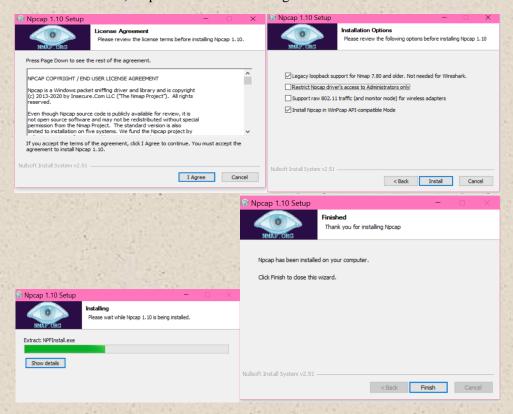


Fig. 22. Instalación de npcap.

3. Se abrió NetBeans IDE y se creó un proyecto nuevo de tipo JAVA WITH MAVEN -> Java Application. Se le puso nombre al proyecto como práctica 1, se dio clic derecho sobre la carpeta "Source Packages" del proyecto recién creado y se eligió la opción New->Java Class. Se creó un nuevo archivo de tipo Java->Java Class y se nombró GetNextRawPacket.java. Se puso el código de java del anexo en el archivo (véase la figura 28).

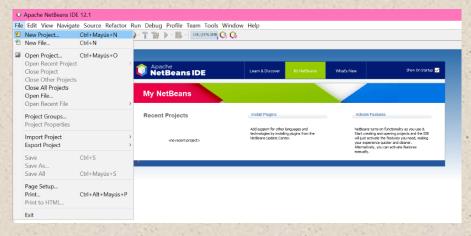


Fig. 23. Creación de nuevo proyecto en NetBeans.

The hint was in Secret that gir

18 les arties o

ce accrue par un assie. ai deja separe leurs talents

e vaistuage de Cesar les | à metire

araissent un peu trop vient des antres

d. Ce qui vient de soi vant mis

48 Watches, et que la fraicheur est 1. També

nalité superieure, parce qu'on les a pins qu'elles ne se vendent au ma

co par des moyens naturels et ? ptionnel. Il s'agit ici de p'an le s'exprimer ainsi. Le irs, le jardinage de at different; elles con

re foyer. Les cultu

le remplace du m

-che, on ne se ci ci aux vitres e denr art Trete

dit la nair . on et de jus-

Portent

12 8

que les personn

-Trure-

Fig. 24. Selección del archivo Java with Maven y Java Application.

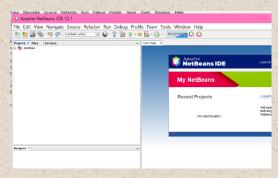


Fig. 25. Nombramiento del proyecto como practica 1.

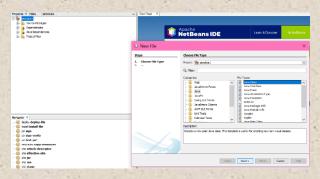


Fig. 26. Creación de la clase de Java.

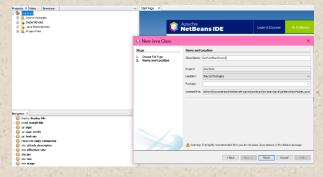


Fig. 27. Nombramiento de la clase como GetNextRawPacket.

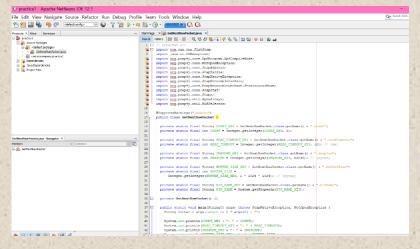


Fig. 28. Poner en el archivo el código.

4. Se añaden las dependencias de la biblioteca pcap4j dando clic derecho en dependencias y seleccionando agregar. Pues en la pestaña de búsqueda de la ventana de dependencias se busca la palabra pcap4j y se agregaron las dependencias encontradas: org.pcap4j-core(1.8.2[jar]central), JNA (net.java.dev.jna), Pcap4j-packetfactory-propertiesbased-1.8.2 y pcap4j-packetfactory-static-1.8.2. (véase la figura 31)

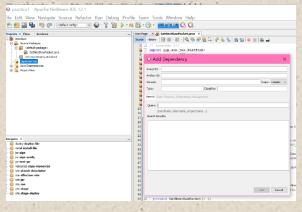


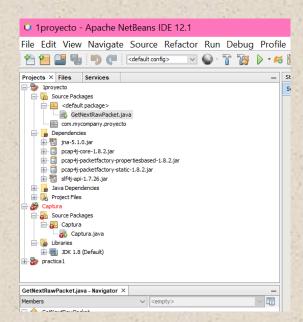
Fig. 29. Adición de dependencias al proyecto.

No.	tPoons IDE	Learn & Discover	My
Add Depender	су		$\times$
Group ID:			
Artifact ID:			
Artifact ID:			
Version:		Scope: compile	~
Type:	Classifier:		
Search Open Projects Depe	ndency Management		
Query: pcap4j			
(coordinate, class na	me, project name)		
Search Results:	,		
			_
a com.ardikars.jxpack	et : jxpacket-pcap-ij et : jxpacket-pcap-ii-spring-boot-autocont	e	^
	non : common-thirdparty.pcap4i.core	ngure .	
iii a org.pcap4i : pcap4i			
⊞- a org.pcap4j: pcap4j	core		
⊕ a org.pcap4j:pcap4j	distribution		
⊕ a org.pcap4j:pcap4j	packetfactory-propertiesbased		
⊞ a org.pcap4j:pcap4j	packetfactory-static		
⊕ a org.pcap4j:pcap4j			
⊕ a org.pcap4j:pcap4j			
ii a org.pcap4j:pcap4j	test-coverage		~
Only 372 of 749 results sh	own. Consider narrowing your search.		
		Add Cano	-1

Fig. 30. Búsqueda de las dependencias de la biblioteca pcap4j.



deur aux vitres che, on ne se de remplace du re foyer. Les culta différent ; elles ce



18 les arties

ce accrue par un ance.

ni dėja sėpare leurs talents

e voisinage de Cesar les à moura

saraissem un peu trop vient des antres.

.d. Ce qui vient de sot vant

Ars Buiches, et que la fraicheur est 1.

nalité superieure, parce qu'on les a plus qu'elles ne se vendent au ma

ces par des moyens naturels et l vitonnel. Il s'agit ici de p'a le s'exprimer ainsi. Le irs, le jardinage de a different; elles co

re foyer. Les culu

le remplace du r

che, on ne se c aux vitres

denr ar

ret

lit la nair on et de jus-

12 8

portent

que les person

-Pliche-

Fig. 31. Todas las dependencias agregadas.

5. Se dio clic derecho sobre el programa GetNextRawPacket.java y se dio clic a la opción del menú contextual "Run" para arrancar el programa y ver el resultado. En la ventana de Salida de NetBeans (Output) se enlistaron las interfaces de red encontradas (véase la figura 33 a) y se eligió la 1 (véase la figura 33 b) pues nos muestra una dirección IP válida (véase la figura 33 c).

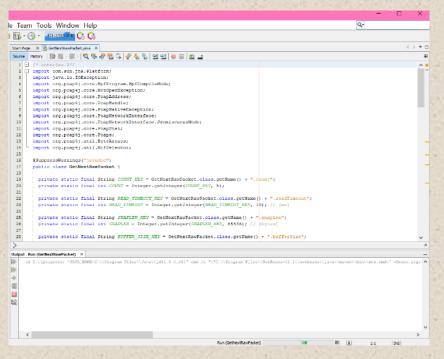
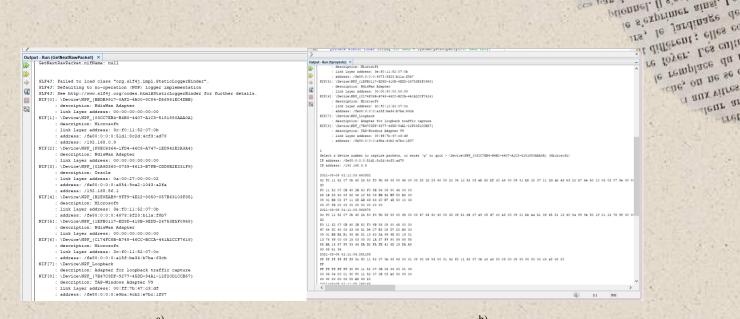


Fig. 32. Ejecución del proyecto.

ablic so dit la paix dans on et de jus- la Remeque les personnages -Plate-pulls down 18 les artistes? Dans re accrue par un artifica in ai deja separe leurs talents e voisinage de Cesar les | à meure au comaraissent un peu trop vient des antres. ce nour an-A. Ce qui vient de soi vaut miene de us malcaes, et que la fraicheur est leur mérile plus qu'elles ne se vendent au m portent ces par des moyens naturels et ptionnel. Il s'agit ici de pla le s'exprimer ainsi. Le



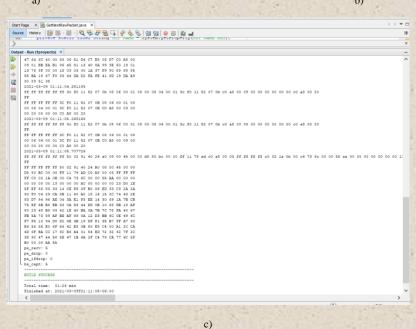


Fig. 33. Resultado de la trama a) y selección de la interfaz de red 1 b) y c) que nos muestra una dirección IP válida.

it aux vitres

alenr ar

TIGI

# 2.11. Funcionamiento del programa

am

EL W portent

Al darle run al programa previamente escrito, este inmediatamente nos va a mostrar en la ventana de salida de Netbeans las interfaces de red encontradas en el sistema. Como se muestra en la siguiente figura:

ce acerno.

ai dejà separe laura

e voisinage de Cesar les

araissent un peu tron vient a

.d. Ce qui vient de

Il's Bolenes, et que la fraiebeau.

nalité superieure, parce qu' plus qu'elles ne se vendent au n ces par des moyens naturels et ptionnel. Il s'agit ici de p'a le s'exprimer ainsi. Le irs, le jardinage d a différent; elles e re foyer. Les cult

le remplace du che, on ne se

d aux vitre

Fig. 34. Selección de la interfaz de red 3 que nos muestra una dirección IP válida también.

Inmediatamente nos permitirá escoger una de las 8 enlistadas (en este caso). Se hizo la selección de la 1 ya que nos mostró una dirección IP válida. Aunque también se pudo haber elegido la numero 3. Se observa que son correctas porque tienen el link layer address y ambos address.

```
2011-03-05 23:26:05.425044
33 33 ff 00 a6 a4 00 00 27 00 00 02 96 dd 60 00 00 00 00 20 3a ff fe 90 00 00 00 00 00 00 a8 54 9c a2 10 43 a2 fa ff 02 00 00 00 00 00 00 00 00 01 ff 00 a6
```

Fig. 35. Resultado del programa donde se muestra la trama a) y b).

Total time: 01:10 min Finished at: 2021-03-09T23:26:05-06:00



3. Conclusiones

#### González Mora Erika Giselle

Se sabe que todos los dispositivos que se encuentran en una red Ethernet se encargan de intercambiar paquetes de datos, estos paquetes reciben el nombre de "tramas Ethernet", un nombre bastante peculiar.

at deia son

e voisinage da over araissent un peu trop

.J. Ce ani vi

Il's Bulgaes, Of and la c

nalité supérienra ....

plus qu'elles ne se vendent es par des moyens naturels et facile. ptionnel. Il s'agit ici de p'antes d le s'exprimer ainsi. Le força urs, le jardinage de tout at different; elles constitu re foyer. Les cultures p le remplace du mieux

che, on ne se croise it aux vitres et au

deur aruffere rrete pas.

anu,

Gracias a esta práctica se comprendió que estas tramas contienen registros de datos muy valiosos para la comunicación de dispositivos a través de la red Ethernet y que estos registros consisten en un código binario que incluye las direcciones MAC destino, MAC origen, tipo de protocolo, información de control, datos, y sumas de comprobación.

También es importante recalcar que las tramas Ethernet tienen un tamaño que va desde los 64 bytes hasta los 1518 bytes y que, si una trama tiene un tamaño menor a los 64 bytes, o sobrepasa los 1518 bytes, el dispositivo receptor descarta esa trama.

Finalmente puedo decir que esta práctica más que difícil fe tediosa. Sin embargo, valió la pena hacer tantos pasos de instalación.

#### Olivares Ménez Gloria Oliva

Con esta práctica pude comprender mejor las tramas con los registros de datos para establecer la comunicación entre dispositivos a través de una red, reforzando así lo visto en clase.

El proceso de instalación fue bastante largo y hubo un poco de problemas durante el mismo.

Una vez que terminé de colocar los directorios de las bibliotecas y de los archivos include e intenté compilarlo, me salían ciertos errores en el registro de compilación.

Al principio no entendí lo que pasaba debido a que había seguido al pie de la letra las instrucciones. Sin embargo, me di cuenta después que el error había sido el compilador, no tenía seleccionado el que era correcto.

Con esto me doy cuenta de que absolutamente todos los pasos cuentan, incluidos los que podrían parecer que no tienen gran importancia, así que podré ser cuidadosa en ese aspecto.

En resumen, la práctica reforzó conocimientos y aunque fue un poco confuso el proceso de instalación al principio, al final todo salió bien.

# 4. Bibliografía

NMAP. (s. f.). Npcap: WinPcap for Windows 10. NMAP.org. Recuperado 9 de marzo de 2021, de

https://nmap.org/npcap/windows-10.html

Trama de Ethernet - Redes de computadoras. (s. f.). Sites Google. Recuperado 9 de marzo de 2021, de

https://sites.google.com/site/sabyrodriguezgamez/unidad-iv/4-2-trama-de-ethernet

lit la nain on et de jus- 1. e. portent que les novembres -Ticre-AS les arties ce accrue par un auto ai deja separe leurs talente 1 e voisinage de Cesar les | à metino straissent un peu trop vient des antres d. Ce qui vient de soi vant .... It's Iruicaes, et que la fraicheur est in nalité supérieure, parce qu'on les a pins qu'elles ne se vendent au mai ocs par des moyens naturels et fa Pilonnel. Il s'agit ici de p'an le s'exprimer ainsi. Le f

```
5. Anexos
```

```
Código c
//interfaz 3
#ifdef _MSC_VER
/*
 * we do not want the warnings about the old deprecated and unsecure CRT
functions
 * since these examples can be compiled under *nix as well
 */
#define CRT SECURE NO WARNINGS
#endif
#include <pcap.h>
/* prototype of the packet handler */
void packet handler(u char *param, const struct pcap pkthdr *header, const
u_char *pkt_data);
int main()
{
      pcap if t *alldevs;
      pcap_if_t *d;
      int inum;
      int i=0;
      pcap t *adhandle;
      char errbuf[PCAP ERRBUF SIZE];
      /* Retrieve the device list */
      if(pcap findalldevs(&alldevs, errbuf) == -1)
      {
            fprintf(stderr, "Error in pcap_findalldevs: %s\n", errbuf);
```

irs, le jardinage de at different; elles con

re foyer. Les cultan le remplace du m

-che, on ne se cr ci aux vitres e

deur art

```
exit(1);
      }
      /* Print the list */
      for(d=alldevs; d; d=d->next)
            printf("%d. %s", ++i, d->name);
            if (d->description)
                  printf(" (%s)\n", d->description);
            else
                  printf(" (No description available)\n");
      }
      if(i==0)
            printf("\nNo interfaces found! Make sure WinPcap is
installed.\n");
            return -1;
      }
      printf("Enter the interface number (1-%d):",i);
      scanf("%d", &inum);
      if(inum < 1 || inum > i)
      {
            printf("\nInterface number out of range.\n");
            /* Free the device list */
            pcap_freealldevs(alldevs);
            return -1;
      }
```

irs, le jardinage de tol at different; elles const re foyer. Les cultures

le remplace du mie

-che, on ne se croi a aux vitres et deur aruffe

```
Monnel. Il s'agit ici de p'ani
                                                                               le s'exprimer ainsi. Le fe
                                                                                irs, le jardinage de l
                                                                                 at different; elles con
                                                                                  re foyer. Les cultur
      /* Jump to the selected adapter */
      for(d=alldevs, i=0; i< inum-1; d=d->next, i++);
      /* Open the device */
      /* Open the adapter */
      if ((adhandle= pcap_open_live(d->name, // name of the device
                                              65536,
                                                                      // portion
of the packet to capture.
                                                                      // 65536
grants that the whole packet will be captured on all the MACs.
                                                                      11
promiscuous mode (nonzero means promiscuous)
                                                                      // read
                                              1000,
timeout
                                              errbuf
                                                                      // error
buffer
                                              )) == NULL)
      {
             fprintf(stderr, "\nUnable to open the adapter. %s is not supported
by WinPcap\n", d->name);
             /* Free the device list */
             pcap_freealldevs(alldevs);
             return -1;
      }
      printf("\nlistening on %s...\n", d->description);
      /* At this point, we don't need any more the device list. Free it */
      pcap_freealldevs(alldevs);
      /* start the capture */
      pcap_loop(adhandle, 15, packet_handler, NULL);
```

re accrue nan

ai déjà sépare leurs tol

e voisinage de Cesar les

arassent un peu trop | vient des

.d. Ce qui vient de soi

It's Bulcues, et que la frainheur

ualité supérieure, parce an'on iplus qu'elles ne se vendent au man

ces par des moyens naturels et fa

le remplace du m che, on ne se cr

it aux vitres e denr arti

111000

on et de in-

portent

que les

oped the

on et de ins-

Portent

que les po-

```
pcap_close(adhandle);
      return 0;
}
/* Callback function invoked by libpcap for every incoming packet */
void packet_handler(u_char *param, const struct pcap_pkthdr *header, const
u_char *pkt_data)
{
      struct tm *ltime;
      char timestr[16];
      time t local tv sec;
      /*
      * unused parameters
       */
      (VOID)(param);
      (VOID)(pkt data);
      /* convert the timestamp to readable format */
      local_tv_sec = header->ts.tv_sec;
      //ltime=localtime(&local_tv_sec);
      //strftime( timestr, sizeof timestr, "%H:%M:%S", ltime);
      //printf("%s,%.6d len:%d\n", timestr, header->ts.tv_usec, header->len);
      int j=0, k=0;
      printf("MAC destino:\n");
      for(j=0;j<6;j++){
         printf("%02X:",pkt_data[j]);
      }
      printf("\n MAC origen:\n");
```

18 les a...

ce accrue nav un

ai deja separe leurs talent

& Vaisnage de Cesar les

araissent un peu trop | vient des anten-

-d. Ce qui vient de soi vani

It's Walcaces, et que la fraicheur oct ;

nalité supérieure, parce qu'on

plus qu'elles ne se vendent au es par des moyens naturels ptionnel. Il s'agit ici de le s'exprimer ainsi. 11'8, le jardinage at different; elle

re foyer. Les le remplace

che, on ne T BUX VI

den

In a chole

for large and a chole

for large

```
irs, le jardinage de
      for(k=6; k<12; k++){}
         printf("%02X: ",pkt_data[k]);
      }
      printf(" \n\n");
    unsigned short tipo = (pkt_data[12]*256)+pkt_data[13];
                       %02X %02X \n",tipo,pkt data[12],pkt data[13]);
    printf("Tipo: %d
}
Código Java
/* interfaz 2*/
import com.sun.jna.Platform;
import java.io.IOException;
import org.pcap4j.core.BpfProgram.BpfCompileMode;
import org.pcap4j.core.NotOpenException;
import org.pcap4j.core.PcapAddress;
import org.pcap4j.core.PcapHandle;
import org.pcap4j.core.PcapNativeException;
import org.pcap4j.core.PcapNetworkInterface;
import org.pcap4j.core.PcapNetworkInterface.PromiscuousMode;
import org.pcap4j.core.PcapStat;
import org.pcap4j.core.Pcaps;
import org.pcap4j.util.ByteArrays;
import org.pcap4j.util.NifSelector;
@SuppressWarnings("javadoc")
public class GetNextRawPacket {
  private static final String COUNT_KEY = GetNextRawPacket.class.getName() +
".count";
```

private static final int COUNT = Integer.getInteger(COUNT\_KEY, 5);

at different; elles ce

re foyer. Les culti le remplace du

che, on ne se c

I aux vitres aleur ar

```
e voisinage de Cesar les | à meure an comme
                                           araissent un pen trop vient des antres : ce neut autre
                                                                irs ir alcaes, et que la fraicheur est leur mérite
                                                                          pins qu'elles ne se vendent au in
                                                                            ocs par des moyens naturels et
                                                                                vitonnel. Il s'agit ici de p'a
                                                                                  le s'exprimer ainsi. Le
                                                                                   irs, le jardinage de
  private static final String READ_TIMEOUT_KEY =
                                                                                    A différent; elles ca
GetNextRawPacket.class.getName() + ".readTimeout";
                                                                                     re foyer. Les cult
                                                                                      le remplace du
  private static final int READ_TIMEOUT =
                                                                                       che, on ne se
Integer.getInteger(READ_TIMEOUT_KEY, 10); // [ms]
                                                                                          a aux vitres
                                                                                            deur a
  private static final String SNAPLEN KEY = GetNextRawPacket.class.getName()
+ ".snaplen";
  private static final int SNAPLEN = Integer.getInteger(SNAPLEN KEY, 65536);
// [bytes]
  private static final String BUFFER SIZE KEY =
GetNextRawPacket.class.getName() + ".bufferSize";
  private static final int BUFFER_SIZE =
      Integer.getInteger(BUFFER_SIZE_KEY, 1 * 1024 * 1024); // [bytes]
  private static final String NIF NAME KEY = GetNextRawPacket.class.getName()
+ ".nifName";
  private static final String NIF_NAME = System.getProperty(NIF_NAME_KEY);
  private GetNextRawPacket() {}
  public static void main(String[] args) throws PcapNativeException,
NotOpenException {
    String filter = args.length != 0 ? args[0] : "";
    System.out.println(COUNT KEY + ": " + COUNT);
    System.out.println(READ_TIMEOUT_KEY + ": " + READ_TIMEOUT);
    System.out.println(SNAPLEN KEY + ": " + SNAPLEN);
    System.out.println(BUFFER SIZE KEY + ": " + BUFFER SIZE);
    System.out.println(NIF NAME KEY + ": " + NIF NAME);
    System.out.println("\n");
    PcapNetworkInterface nif;
    if (NIF NAME != null) {
      nif = Pcaps.getDevByName(NIF_NAME);
    } else {
      try {
         nif = new NifSelector().selectNetworkInterface();
      } catch (IOException e) {
```

-ublic se tra

lit la paix dans

on et de jus- la fleure roin.

e.printStackTrace();

portent que les personnages

-Place - As dorvort .

18 les artistes? Dans re accrue par un artifice in-

ai deja separe leurs talents | la nimas.

d. Ce qui vient de soi vaut mieux diten-

CHENTS dit la pair d on et de jus-12 800 que les personne - - Trute--118 M 18 les artistans n ce accrue par un swie at dejà separe leurs talems d Voisinage de Cesar les | à metro au araissent un peu trop vient des antres. d. Ce qui vient de soi vant mi-Contracts, et que la fraicheur est leur a Portent pins qu'elles ne se vendent ocs par des moyens natur ptionnel. Il s'agit ici

```
return;
  }
  if (nif == null) {
    return;
}
System.out.println(nif.getName() + " (" + nif.getDescription() + ")");
for (PcapAddress addr : nif.getAddresses()) {
  if (addr.getAddress() != null) {
    System.out.println("IP address: " + addr.getAddress());
  }
}
System.out.println("");
PcapHandle handle =
    new PcapHandle.Builder(nif.getName())
        .snaplen(SNAPLEN)
        .promiscuousMode(PromiscuousMode.PROMISCUOUS)
        .timeoutMillis(READ TIMEOUT)
        .bufferSize(BUFFER SIZE)
        .build();
handle.setFilter(filter, BpfCompileMode.OPTIMIZE);
int num = 0;
while (true) {
  byte[] packet = handle.getNextRawPacket();
  if (packet == null) {
    continue;
```

le s'exprimer air irs, le jardina

d different; re foyer, Le

le remplac che, on

```
} else {
    System.out.println(handle.getTimestamp());
    System.out.println(ByteArrays.toHexString(packet, " "));
    for(int j=0;j<packet.length;j++){</pre>
        System.out.printf("%02X ",packet[j]);
        if(j\%16==0)
            System.out.println("");
    }//for
      System.out.println("");
    num++;
    if (num >= COUNT) {
      break;
    }
PcapStat ps = handle.getStats();
System.out.println("ps_recv: " + ps.getNumPacketsReceived());
System.out.println("ps_drop: " + ps.getNumPacketsDropped());
System.out.println("ps_ifdrop: " + ps.getNumPacketsDroppedByIf());
if (Platform.isWindows()) {
  System.out.println("bs_capt: " + ps.getNumPacketsCaptured());
handle.close();
```

e s'exprimer ainsi. irs, le jardinage

at différent; elles re foyer. Les c

le remplace d che, on ne